GNB RSA Token Standards and Procedures

Client Authentication Standards

Concept

The client authentication standard provides a formalized, secure and efficient methodology for proper identification of the RSA Token User, and subsequent binding of the token to the identified Token User.

Two different token types are available:

RSA Hardware Token (key fob)

RSA Blackberry Token (Software Application)

The term "RSA Token" referenced throughout this document refers to both token types. At times only one token type is referenced, and this will be indicated by stating either "RSA Hardware Token" or "RSA Blackberry Token".

RSA Tokens shall be used to provide a form of two factor authentication capability within GNB. These RSA Tokens shall be available to:

- All GNB departments and applicable Crown Corporations
- All government staff
- Contractor or consultant

Any Information Technology applications requiring a form of two factor authentication services.

Concept
(continued)

The RSA Token system has been designed by GNB to provide an assurance level of "**Medium**" and is thus suitable for use with data of that classification or lower.

GNB has chosen a management concept for the RSA Hardware Tokens which allows the departments to self manage their token inventory and distribution. In this framework departments are issued a bulk inventory of hardware tokens as needed and will distribute them as appropriate within the standard processes structure as outlined herein.

RSA blackberry software tokens are still purchased in bulk by departments however they are still managed centrally and distributed directly to end users by the RA.

The standards and procedures are established to assist in control of the RSA Tokens for the protection of the reputation of the Token User who is accessing resources within the government of New Brunswick network.

Roles and Responsibilities

Secure control of RSA Tokens remains the responsibility of four entities:

- **Registration Authority** (RA) for central system registration, activation and batch distribution of the RSA Tokens to the departments as well as authorization of RSA Token requests.
- **Local Registration Authority (LRA)** for maintaining departmental token inventories and procedures for RSA Token management, processing token requests and facilitating delivery of tokens to the Token User.
- **Managers/Signing Authorities** for initiating requests for tokens, for the identification of the Token User and supervision of the registration process.
- **Token User** for **effective** use and protection of the RSA Token.

Background

GNB has chosen RSA Tokens to provide formal secure two factor authentication. RSA Tokens will be used to provide secure authenticated access to various resources within the GNB network.

Standard

As a basic principle, RSA Token registration and use shall adhere to a series of standards that protect the initialization, distribution, operation, and disposal of RSA Tokens.

- RSA Token request forms must:
  - Be properly filled out before the LRA can initiate a token activation.
  - Include a departmental Managers/Signing Authorities signature as formal acknowledgement of responsibility for requesting the RSA Token.
  - Include the signature of the Token User as formal acknowledgement of their agreement to the "GNB RSA Token User Terms and Conditions" document.
  - Include the signature of any departmental administrative staff or proxies who have participated in the RSA Token activation; this would include the Primary LRA, the Secondary LRA, and any CRI's or Designated Professionals.
  - Be retained by the Departments, both initial requests and change requests, as individual records.
  - Only be accepted from LRAs, and shall be sent via encrypted email to the RA.
- Each Token User must be properly identified via:
  - **Physical recognition** if the individual is **well** known to the LRA, CRI, or Designated Professional (For an employee you have worked with for many months, and you know is the person identified on the form, you can select "Working Relationship" as the verification).
  - **Or** by **viewing 2 pieces of ID documents** from the Token User, at least one which must be a picture ID (The LRA may designate the Token User's manager or another trusted designate to perform physical identification.).
- RSA Token requests are processed by **Registration Authority** during the normal work hours.
- All RSA Token requests received by the Registration Authority shall be completed within 2 work days for normal requests completion.

Continued on next page

Standard
(continued)

- The RSA Token inventory is a department responsibility (Primary LRA) and shall be properly protected at all times.
- Individual tokens for users shall be distributed to only the appropriate LRA, CRI or if necessary Designated Professional.
- It is recommended that departments audit their RSA Token use on a 6 month basis to identify and deactivate any tokens no longer in use.
- The RA will audit activated RSA Tokens that remain in new-pin mode and notify the appropriate LRA on a bi-weekly basis.
- All Token Users:
    - Are required to read and adhere to RSA Token control methodology as described in the "GNB RSA Token Usage Terms & Conditions" document.
    - Must protect their RSA Token from loss or personal (PIN) Number disclosure and is not permitted to share it with anyone within or outside government under any circumstances.
    - Have the ability to reset a forgotten PIN if they have completed the Q&A Authentication portion of the registration process. This reset functionality is deemed acceptable based on the premise that all lost or compromised tokens are reported immediately to the RA or LRA.

Client Authentication and Registration Procedure

GNB currently uses RSA Tokens for following purposes:

- IPSec remote access (VPN)
- SSL remote access (SSLVPN)
- Wireless authentication
- PDAS (Private Dialup Access System)

In order to guarantee the RSA Token can be trusted the token must be issued in a manner that will bind the RSA Token to the identified Token User. It is imperative that all efforts be made to properly identify the Token User. Following this "Client Authentication and Registration Procedure" for the issuance of RSA Tokens will ensure an appropriate level of confidence in binding a token to the correct Token User.

PART 1 - RSA Hardware Token - Client Authentication and Registration Procedure

Agent	Action
Manager / Signing Authority	1. Identify the need for a user to have remote access to the GNB network. 2. Complete the "Secure Remote Access Token Request Form" in electronic format (The form may be filled in by the LRA if they have access to the required personnel information). 3. Save this form as a word document. 4. Print and sign the form (in Blue Ink), and send the original form (not photocopy) to the LRA through interoffice mail. The form MUST be signed by the appropriate manager (Signing Authority). 5. Email the electronic copy of the form to the LRA.
LRA	6. Remove an unassigned token from inventory and enter the token serial number in the "Token Specifications" section of the "Secure Remote Access Token Request Form". 7. Submit the form, via Secure Email, to "(GNB) Token Administrators" or gnbtokenadministrators@gnb.ca

RA	8. Receive the "Secure Remote Access Token Request Form" form via Secure Email, and input the following information into the RSA Web Express web site: • Token Type: Key fob • User ID: Must match the users Active Directory User ID • First Name • Last Name • Email address: Must match the users email address **Note: All data must be entered exactly as it is shown on the form.** 9. Perform any accounting functions as required: • ACS entries • Billing Web Application 10. Approve the request in the RSA Web Express web site. This action sends an email to the Token User containing the following 4 items: • A Token Activation Code • Instructions on how to activate the token (once received) • Instruction that the token will be delivered by their LRA or designate within a few days. • Procedure for lost token or token re-issue. 11. Reply back to the original request from the LRA in step 7, via Secure Email, informing them the request has been successfully processed and that a token can now be issued to the Token User.
LRA	12. Decide who will deliver the token to the Token User: • The LRA delivers the token • The LRA sends the token & original copy of the form through interoffice mail to a CRI or Designated Professional who delivers the token

LRA, CRI or Designated Professional	13. Authenticate the Token User personally. Complete the "Local Registration" section of the "Secure Remote Access Token Request Form" & give the Token User copies of / or links to: • GNB RSA Token Usage Terms & Conditions • RSA Web Express User Guide 14. Sign and date the original "Secure Remote Access Token Request Form" with the current date (using blue ink only). **Note:** If a CRI or Designated Professional completes this step then it must be sent back to the LRA through interoffice mail. 15. Retain this form in the Records Management Area. **Note:** Corporate Records Management staff suggests these forms should be filed under CPRS 1755-01. CPRS 1755-01 has a retention period of A=SO, SA=0, FD=D, which translates to "kept in the office Records Management area until superseded or obsolete, and then destroy". 16. Coach the user through the token registration process to ensure that it is fully completed in a timely manner. • Activation – Steps 17 to 18 • Set-pin – Steps 19 to 21 • Q&A setup – 22
Token User	17. Read the documentation that is provided. • GNB RSA Token Usage Terms & Conditions • RSA Web Express User Guide 18. Visit the RSA Web Express web site: (https://gnb-rsa-webexp.gnb.ca/RSASWE/WXUserHome.do) and input information required to activate their token. If the Token User selects the link in the email sent to them in step 9 the only information required for input is the token serial number: • User ID - Must match the users Active Directory User ID • Token Activate Code – This is the email sent to the Token User in step 9 • Token Serial Number – 9 digit number located on back of token right above the expiry date

Token User	19. When the "Token Activation Complete" message is displayed, select "Test Your Token" and input the following information: • User ID - Must match the users Active Directory User ID • Token Passcode – The 6 digit number displayed on the token 20. Follow the on screen instructions to create a PIN 21. When the "PIN Change Complete" message is displayed, select "Home" to return to the main menu and then select "Test Your Token". Login with the new PIN using the following information: • User ID - Must match the users Active Directory User ID • Token Passcode – <users 4-8 character alphanumeric PIN> + the 6 digit number displayed on the token (Example your pin is "abc123", so enter "abc123XXXXXX" where the X's represent what is displayed on the token). **IMPORTANT:** You cannot use the same 6 digits that were used in step 19 above, if necessary wait until the token displays a new 6 digit number. **The Token is now activated in the users name and can only be used for remote access in conjunction with the PIN that only the Token User knows.** 22. Still within the RSA Web Express web site, click "Home" to return to the main menu and then select "Set up Q & A Authentication". The system will ask the Token User to provide 5 easy to remember questions / answers. **Should a Token User forget their PIN they can go back to the RSA Web Express web site anytime and reset their PIN after correctly answering any 3 of the 5 preset questions.**

PART 2 - RSA Blackberry Token - Client Authentication and Registration Procedure

Agent	Action
Manager / Signing Authority	1. Identify the need for a user to have remote access to the GNB network. 2. Complete the "Secure Remote Access Token Request Form" in electronic format (The form may be filled in by the LRA if they have access to the required personnel information). 3. Save this form as a word document. 4. Print and sign the form (in Blue Ink), and send the original form (not photocopy) to the LRA through interoffice mail. The form MUST be signed by the appropriate manager (Signing Authority). 5. Email the electronic copy of the form to the LRA.
LRA, CRI or Designated Professional	6. Authenticate the Token User personally and complete the "Local Registration" section of the "Secure Remote Access Token Request Form" & give the Token User copies of / or links to: • GNB RSA Token Usage Terms & Conditions • RSA Web Express User Guide 7. Sign and date the original "Secure Remote Access Token Request Form" with the current date (using blue ink only). **Note:** If a CRI or Designated Professional completes this step then it must be sent back to the LRA through interoffice mail. 8. Retain this form in the Records Management Area. 9. **Note:** Corporate Records Management staff suggests these forms should be filed under CPRS 1755-01. CPRS 1755-01 has a retention period of A=SO, SA=0, FD=D, which translates to "kept in the office Records Management area until superseded or obsolete, and then destroy".
LRA	10. Submit the form, via Secure Email, to "(GNB) Token Administrators" or gnbtokenadministrators@gnb.ca

RA	11. Receive the "Secure Remote Access Token Request Form" form via Secure Email, and input the following information into the RSA Web Express web site: • Token Type: Blackberry software token • User ID: Must match the users Active Directory User ID • First Name: "<firstname> (bberry)", ex: "John (bberry)" • Last Name: "<lastname> (bberry pin #)", ex: "Smith (12345678)" • Email address: "noemail" (Field can't be blank but no email is required as deployment is manual) **Note: All data must be entered exactly as it is shown on the form.** 12. Perform any accounting functions as required: • ACS entries • Billing Web Application 13. Reply back to the original request from the LRA in step 10, via Secure Email, informing them the request has been successfully processed and that the Token User will receive an email containing the software token and instructions on how to install it.
Token Creator (RSA System Administrator)	14. Approve the request in the RSA Web Express web site 15. Hard codes the GNB label and the Blackberry PIN to the software token file 16. Re-issues the software token 17. Emails Token User, attaching the software token file and instructions on how to import it into their blackberry device.
LRA, CRI or Designated Professional	18. Coach the user through the token testing and registration process to ensure that it is fully completed in a timely manner. • Initial Authentication Test – Steps 19 to 20 • Set-pin – Steps 21 to 22 • Q&A setup – 23

Token User	19. Read the documentation that is provided. • GNB RSA Token Usage Terms & Conditions • RSA Web Express User Guide 20. Visit the RSA Web Express web site: (https://gnb-rsa-webexp.gnb.ca/RSASWE/WXUserHome.do) and select "Test your token", and at the prompt enter your User ID and Passcode (On your Blackbrry select "Get Passcode" and enter the 8 numbers displayed on the screen). 21. Follow the on screen instructions to create a PIN 22. When the "PIN Change Complete" message is displayed, select "Home" to return to the main menu and then select "Test Your Token" again. Login with the new PIN using the following information: • User ID - Must match the users Active Directory User ID • Token Passcode – The Passcode is generated by opening the RSA application on your Blackberry, entering your pin, and then selecting "Get Passcode". **IMPORTANT:** You cannot use the same 8 digits that were used in step 20. **The Token is now activated in the users name and can only be used for remote access in conjunction with the PIN that only the Token User knows.** 23. Still within the RSA Web Express web site, click "Home" to return to the main menu and then select "Set up Q & A Authentication". The system will ask the Token User to provide 5 easy to remember questions / answers. **Should a Token User forget their PIN they can go back to the RSA Web Express web site anytime and reset their PIN after correctly answering any 3 of the 5 preset questions.**

RSA Token Information Changes

There will be circumstances that require changes to an individual's information associated with a RSA Token, such as an employee name change, employee status change, or the addition of secure access to another system. If a Token Users information or access restrictions needs alteration, following the "Procedures for RSA Token changes" will help maintain the accuracy of the information associated with each RSA Token and proper billing of the services.

Procedures for RSA Token changes

Agent	Action
Token User	1. Identify the need to have their registration information updated.
Manager / Signing Authority	2. Follow the same procedures as steps 2 through 5 in the "Client Authentication and Registration Procedure" section, noting in the comments area what information change(s) are required.
LRA	3. Submit the form, via Secure Email, to "(GNB) Token Administrators" or gnbtokenadministrators@gnb.ca
RA	4. Implement any required changes (The RA may need to coordinate with the RSA System Administrator depending on the nature of the changes). 5. Communicate to the LRA that the requested changes have been completed.
LRA	6. Communicate to the Token User that the requested changes have been completed. 7. File the original "Secure Remote Access / Token Request Form" in a secure location, in the Records Management Area. These files are not to be destroyed.

Lost Tokens / RSA Token Re-issue

Lost tokens, tokens with hardware failures and forgotten personal (PIN) numbers (failed reset via Q&A) will require the current RSA Token be deactivated by filling in a "Token Deactivation Request Form" and a NEW RSA Token be requested by following the "Initial Registration Procedures for Issuance of RSA Tokens" procedures above.

Important Note: If the RSA Token is lost or stolen, the Token User is to try and contact the LRA immediately to report it. If the LRA is not available, the Token User is to call the CIMS help desk at 506-444-2467 to report the lost or stolen RSA Token so that it can be deactivated as soon as possible.

There can be a variety of circumstances where a Token User's RSA Token is lost, damaged or the personal (PIN) Number is forgotten and a re-issue is required. The circumstances that can contribute to requiring a re-issue of RSA Tokens include:

- the Token User has lost their RSA Token or had it stolen
- The token is non-functioning
- Token User has left his/her position or changed departments

These would also apply if the user has not completed the "Q & A Authentication" or cannot remember the answers to 3 of the 5 questions needed to identify themselves to the RSA Web Express System:

- the Token User has forgotten their personal (PIN) number
- the Token User suspects that their personal (PIN) number has been compromised

RSA Token re-issues, because of a forgotten PIN, can become counter-productive to efforts in increasing the client understanding of the importance of protecting their token and associated personal (PIN) number. The basic principle is that the RSA Token re-issue procedure will always be more effort than the requirement to remember the personal (PIN) Number in the first place.

The following steps are suggested:

1. Investigate the incident in some detail.
2. Identify and document any causes contributing to the requirement for a RSA Token re-issue. Ensure this information is included in the Reason for Deactivation section of the "Request for Deactivation" form.
3. Insure the Token User's management is made aware of the problem.

Base Procedures for RSA Token Re-issue

Agent	Duties
LRA	1. Retrieve the RSA Token. 2. Complete the "Token Deactivation Request Form". 3. Request a new RSA Token be issued to the Token User by following the "Initial Registration Procedures for Issuance of RSA Tokens" procedures above. Note: Retrieved token may be reissued to the same user provided "Initial Registration Procedures for Issuance of RSA Tokens" are followed.

LRA & LRA Proxy Roles

Hardware token Authentication and Administration remains the responsibility of the departmental LRA. However departments may separate the individual steps to allow a Proxy to perform much of the administrative effort. There are three choices for selecting an individual to provide proper identification of the Token User:

1. The first and preferred choice is the use of the **trained LRA staff**.
2. The second choice is the use of a **carefully selected CRI** who can act as a proxy.
3. The final choice is the use of a "**Designated Professional**" in those distant locations where neither of the other choices is available.

It is the Primary LRA who will have to justify this selection based on the need to maintain a high degree of confidence in the LRA registration process, to the satisfaction of all GNB departments.

Roles

Primary LRA – Manages the departmental RSA Token environment:

- Must be a departmental employee with adequate departmental knowledge to properly qualify all RSA Token requests. (Departments are allowed up to 3 LRA's.)
- Maintains departmental token inventory.
- Authenticates, manages and helps train Secondary departmental LRA's.
- Requests all RSA Token updates, Secondary LRA and Proxy staff are not permitted to do this
- Maintains paper record of all transactions.

Secondary LRA – Assists the Primary LRA to authenticate and manage RSA Token Users:

- Does not maintains departmental token inventory, but will be issued individual tokens from the Primary LRA for issue to Token Users
- Fully trained in the LRA role.
- May be a local resource or stationed in a regional office.
- May be departmental employee or contractor.
- May be technically oriented or business support staff.

Proxy–responsible individual who can act as a Proxy for the LRA:

- Limited to use as an LRA proxy at remote locations where there is no LRA
- Untrained in the LRA role
- The Proxy must not perform LRA duties without direction. The LRA will contact the Proxy every time and specify what actions are required.
- Proxy will be either a CRI (Client Responsible Individual) OR a Designated Professional

Proxy Role

The LRA (Primary or Secondary) will be required to coach the Proxy through the form completion and Token User authentication process to insure each duty item is properly completed.

The Proxy must properly fill in and sign the forms as the LRA does. These forms must be properly sealed in an envelope and forwarded via surface mail to the LRA. The LRA must then co-sign these forms.

It has been suggested that the CRI can photocopy the identification documents used in the client identification process, provided they carefully remove all privacy related information from the document (i.e. birth date, drivers licence no., social insurance number). This addition is at the discretion of departmental management and is not required unless the department would like the added assurance that all identification efforts have been performed properly.

CRI– Client Responsible Individual:

- Responsible employee who can act as a Proxy for the LRA:
- Must be well known and trusted by the LRA
- Limited to use as an LRA proxy at remote locations where there is no LRA
- Untrained in the LRA role
- The CRI must not perform LRA duties without direction. The LRA will contact the CRI every time and specify what actions are required.

Designated Professional:

1. A member of a professional association or guild that has a code of ethics governing the honesty and professionalism of the work performed.
2. A Notary Public or others where their honesty and professionalism are guaranteed via the Oath of Office they adhere to.
3. Others who are qualified to assure the identity of the Token User, for example anyone who can corroborate for a passport application.

There are also several characteristics that should be avoided in selection of the Designated Professional:

1. If possible, avoid the selection of other individuals from the same project team or peer group within the office. (The opportunities for collusion should be minimized.)
2. If possible, avoid the immediate team lead, supervisor, or manager. (Again this should help reduce the chance of collusion occurring.)
3. If possible, avoid the selection of office secretarial or administrative staff that don't have a special certification and associated code of ethics to follow. (It is the specific code of conduct or ethics program that binds members of professional associations or guilds. Without ethics or conduct requirements, the opportunities for penalty for illicit behaviour are reduced.)

Glossary

Roles

Management – Departmental line management, signing authority (at the department's discretion) responsible for:

- Authorizing and paying for the RSA Token to be used by the Token User
- Identifying and removing inactive or terminated Token Users

Token User – Departmental Client who will be using the RSA Token

RA – Registration Authority, central RSA Token administrator:

- Manages and implements all RSA Token requests.

LRA – Local Registration Authority, departmental representative:

- Completes the Token User identification.
- Assists the Token User in the completion of the RSA Token installation process.
- Will be appointed at the discretion of the department.
- Will be designated as either a **Primary** or **Secondary** LRA depending on their function within the departmental structure.
- Will be required to undergo a yearly Security Check as part of the full implementation of a production RSA Token distribution process.
- Submits requests for removal of inactive or terminated accounts.

Proxy – Responsible individual who can act as a Proxy for the LRA at remote locations.

- Client Responsible Individual, departmental employee is the preferred approach
- Alternatively may be a trusted "designated professional" at a remote location.

Terminology Clarification

Identification – Face to face evaluation of Token User and their identity documents

Authentication – Electronic identification of Token Users via 2 factor identification method, the Token Users personal (PIN) number and their RSA Token one time password.

Authorization – Interface with the Authentication results to provide appropriate application access via the Token Users security group and level access rights