# NRoSS Participant Access Rights and Authentication Policy

## A. General Access Rights Policy

1. The following terminologies shall be used in defining the Access Rights and Authentication Policy of NRoSS:

1.1 Participant - an entity allowed access to the NRoSS system
1.2 Users - are individuals designated by the Participant to access the NRoSS system
1.3 Participant or User Details - pertains to the information required by BTr to establish the identity of the User or Participant
1.4 User Profile - pertains to the functions in the NRoSS System that can be accessed by a Participant
1.5 NRoSS User Administrator - shall also be referred to as User Admin and shall be performed by the BTr-Scripless Securities Registration Division (BTr-SSRD)
1.6 NRoSS System Administrator - shall also be referred to as Sys Ad and shall be performed by BTr-Systems Administration Division (BTr-SAD)
1.7 Participant Access Rights and Authentication Administrator (PA) - shall also be referred to as “Participant Admin” and designated by the Participant to oversee the proper management and compliance of the access and authentication rights of NRoSS
1.8 e-token - consist of the physical token and the digital certificate
1.9 NRoSS - pertains to the new RoSS System

2. A Participant to NRoSS must obtain the following to access the NRoSS:

2.1. All Users of the Participants must receive a security clearance and must be identified to the NRoSS application before logging on. An e-token containing the digital certificate which serves to authenticate the identity of the User shall be required from each User to log into the NRoSS. The e-token shall be created and managed by the NRoSS System Administrator.

2.2. Each Participant shall likewise be assigned a User Profile to access the various functionalities of the NRoSS System. The User Profile assigned to a Participant shall be based on the group or Investor Type of the Participant. The User Profile shall be assigned/created and managed by the NRoSS User Administrator. Access to NRoSS shall only be allowed on business days within the timeframe stipulated by BTr.

3. If a Participant is unable to access the NRoSS from their own premises the Participant shall abide by the stipulated BCP Plan of the BTr.

## B. User Identification and Authentication

1. User identification and authentication in NRoSS involves two processes:

1.1 Use of e-token and token Password to access the network

1.2 Use of a Username and Password to access the NRoSS application

2. Creation of Username

2.1 Username must be unique to the User and will be associated with the Participant that enrolled him.

2.2. Shall be created by NRoSS User Administrator based on the following convention:

2.2.1. Short name of Participant - maximum of 4 characters

2.2.2. Role or Investor Type of the Participant (e.g. “d” is dealer and “b” is broker

2.2.3. Initials of the User - maximum of 3 characters

2.2.4. Order of creation - from 01 onwards

2.3. The Username shall be used in the creation of the User profile and digital certificate in the e-token.

3. Creation and Maintenance of Password

3.1 There are two types of Password that will be created for the Users of NRoSS namely:

| TYPE | NRoSS ADMINISTRATOR | FUNCTION/USE |
|---|---|---|
| e-Token Password | NRoSS System Administrator | To access network |
| NRoSS Application Password | NRoSS User Administrator | To access NRoSS application |

The NRoSS User Administrator shall initially create the NRoSS Application Password for the Users to access the NRoSS application while the NRoSS System Administrator shall initially create the e-token Passwords for the Users to access the network. These passwords shall be immediately replaced by the User upon initial log into the system.

The e-token Password shall also be created by the NRoSS System Administrator for the Participant Access Rights and Authentication Administrator (i.e., Participant Admin) to enable the Participant Admin to reset the e-token Passwords of the Users.

3.2 The Password of the User must be changed every 30 days. The User must ensure that it maintains 2 different passwords to access the network and NRoSS application.

3.2.1 The maximum number of failed log-in attempts before an account is locked-out is 5x for both the e-token and NRoSS Application Passwords while the maximum failed log-in attempt for the Participant Administrator (PA) of the e-token Password is 15x.

3.2.2 In case the User experiences an “Account Locked-out”, the following process shall be followed:
3.2.2.1 NRoSS application - NRoSS User Administrator shall be responsible for re-setting the RoSS application password of the User.
3.2.2.2 Network - the Participant Administrator (PA) shall be responsible for re-setting the e-token Password of its Users unless the PA experiences an account locked–out and in this instance, the token will have to be presented by the User to the NRoSS System Administrator to reset the Password.

3.3. Disclosure of Passwords is prohibited. Participants are required to enforce these prohibitions.

3.4. The Password must also have the following characteristics:
3.4.1 Must be at least 8 characters in length and consist of at least three password complexities (e.g. mixture of upper and lower case letters and digits or symbols
3.4.2 User must type in the same way the upper or lower case letters.
3.4.3 Must not contain the following:
3.4.3.1 Repetitive letters
3.4.3.2 Use of Username, your own real name or family names
3.4.3.3 Use of the word “, P@$$w0rd”
3.4.3.4 Use previous password
3.4.3.5 Must not contain blank spaces.

## 4. e-token Usage and Management

4.1. The e-token consist of the physical token and the digital certificate that will enable the User to access the infrastructure or network. The e-token shall be inserted into the NRoSS workstation to log in.

4.2. Digital Certificate shall be used to authenticate Users to NRoSS and to digitally sign certain electronic messages transmitted to the NRoSS. No other use is permitted.
4.3. The Users must observe the following rules in using the e-token:

4.3.1. The e-token may only be inserted into a computer/laptop designated as NRoSS workstations and shall only be used to enter the NRoSS application. Users are prohibited from using any other e-token and Username to enter the NRoSS application or sharing their e-token or Username with anyone.

4.3.2. There shall only be one digital certificate created per User and one digital certificate per token.

4.3.3. Use of e-token constitute acceptance by Participant to the terms and conditions of the Participation Agreement.

4.3.4. The digital certificate expires for a period indicated in the digital certificate information and the Participant is responsible for tracking the expiry dates of its digital certificate and applying for a new digital certificate. A token may be re-used for another User of the Participant provided that the digital certificate of the previous User has been revoked.

4.3.5. Participants must report key compromise to the e-token as soon as possible such as lost or stolen e-token. The Participant must observe proper security measures to ensure that the e- tokens are properly used and kept secure by its Users.

4.3.6 Every Participant shall assign a Participant Access and Authentication Rights Administrator (PA) who shall be responsible for the administration of all their NRoSS e- tokens aside from access rights of the Users. The PA shall be responsible for the following:

4.3.6.1. Installs the Gemalto Client Software to the User's laptop or computer.
4.3.6.2. Changes/reset/unlock a User's e-token if the User forgets his token password.
4.3.6.3. Evaluates any change request related to the authentication of the User and ensure compliance to the Token Rules.

4.4. BTr, as system operator, shall likewise designate its NRoSS Systems Administrator to issue and manage the e- tokens as follows:

4.4.1 Creation /revocation/renewal of the digital certificate
4.4.2. Logs and maintains the Registry containing the digital certificates and tokens issued
4.4.3. Deployment of the e-token Kit to Participants and replacement of tokens
4.4.4. Implement the policies and procedures on token management

4.5. The Operating Procedures in the Management of Digital Certificate

4.5.1. Issuance of Digital Certificate

4.5.1.1. A digital certificate shall be issued under the following instances:

4.5.1.1.1. Newly approved Participants
4.5.1.1.2. Renewal of digital certificate
4.5.1.1.3. Replacement of token
4.5.1.1.4. e-token has been shared or compromised
4.5.1.1.5. User Password and Participant Administrator (PA) Password have been locked

4.5.1.2. For Newly Approved Participant, a Participant must execute and comply with all terms and conditions of the Participation Agreement and submit the User Enrollment Form and pay the necessary fees to enroll its various users.
4.5.1.2.1. The NRoSS User Administrator shall create the Participant and Individual User Details and the User Profile per User based on the User Enrollment

Form submitted by the Participant. The NRoSS User Administrator shall also create the Username and initially create the NRoSS Application Password of the User of the Participant.

4.5.1.2.2. The NRoSS Systems Administrator shall create the e-token Password and digital certificate for the User and the Participant Administrator and install the digital certificate to the token.
4.5.1.2.3 The NRoSS System Administrator shall be responsible for distributing the tokens personally to the Users or to the authorized representative of the Participant and the CD installer to the Participant Administrator (PA) or to the authorized representative of the Participant. He shall also be responsible for scheduling the renewal and distribution of the tokens.

4.5.1.3. Renewal of Digital Certificate

4.5.1.3.1. A Participant shall submit a Change Request Form to NRoSS User Administrator to issue a new digital certificate within the prescribed period set by BTr (e.g. one month before expiry date of the digital certificate). The NRoSS User Administrator shall evaluate the Change Request Form in terms of the following: 1) information provided; 2) approving authorities; 3) status of the Participant (e.g. active, suspended or terminated) to determine whether the User is eligible for renewal of the digital certificate.

4.5.1.3.2. A Participant who has been disabled or removed from the NRoSS System within the period set for renewal shall not be allowed to renew the digital certificate of its Users.

4.5.1.3.3. The NRoSS User Administrator shall be responsible for endorsing to NRoSS Sys Ad the renewal of the digital certificate. The NRoSS System Administrator shall create a new digital certificate and e- token Password using the same Username of the User.

4.5.1.3.4. The Users shall bring its token personally or have the authorized representative of the Participant go to the NRoSS System Administrator within the time specified by it to have the new digital certificate installed in the token.

4.5.1.4. Replacement of Token or Security Compromised

4.5.1.4.1 A Change Request Form for the replacement of the token shall be submitted by Participant to NRoSS User Administrator. The replacement of token involves the revocation of the old digital certificate and the issuance of a new digital certificate.

4.5.1.4.2. Where the security is compromised or the e-token has been shared, a change request shall involve the request for the issuance of a new digital certificate.

4.5.1.4.3. The NRoSS User Administrator shall evaluate the Change Request Form in terms of the following: 1) information provided; 2) approving authorities; 3)

status of the Participant (e.g. active, suspended or terminated) to determine whether the User or Participant is eligible for the issuance of a new digital certificate.

4.5.1.4.4. A Participant who has been disabled or removed from the NRoSS System within the period set for renewal shall not be allowed to replace the token or obtain a new digital certificate for its Users.

4.5.1.4.5. The NRoSS User Administrator shall be responsible for endorsing the replacement and or renewal of the digital certificate to NRoSS Sys Ad. The NRoSS Sys Ad shall install a new digital certificate and create a new e-token Password using the same Username of the User.

4.5.1.4.6. The Users shall bring the token personally or have the authorized representative of the Participant go to NRoSS Sys Ad within the time specified by it to have the new digital certificate installed in the token.

4.5.2. Revocation of Digital Certificate

4.5.2.1. A revocation of a digital certificate for individual users may be initiated by the Participant or the BTr in cases where the Participant has been suspended or terminated to access the NRoSS System based on grounds set in the Registry Rules or other pertinent operating rules and procedures of RoSS.

4.5.2.2. A Participant must submit the Change Request Form to the NRoSS User Administrator to revoke a digital certificate of one of its Users. In the case of a Participant who has been terminated by BTr, the NRoSS User Administrator shall write a memo to the NRoSS Sys Ad instructing them to terminate all the Users of the Participant indicating their names and Usernames.

4.5.2.3. The approving officer of NRoSS User Administrator shall approve the revocation of the digital certificate under the following instances:
4.5.2.3.1. The User has resigned or no longer an employee of the participant or transferred to another department

4.5.2.3.2. Security has been compromised (e.g. known to another party)

4.5.2.3.3. The Participant has been terminated by BTr in accordance with the grounds set in the Registry Rules.

4.5.2.3.4. The digital certificate has expired.

4.5.2.3.5. The e-token was lost.

A revocation of the digital certificate shall render the old digital certificate cancelled. A new digital certificate may be created in the name of the old or new Individual User provided the Participant has not been terminated at the initiative of the Participant or BTr.

4.5.2.4. The Change Request Form shall be evaluated by the NRoSS User Administrator in terms of the following: 1) information provided; 2) approving authorities; 3) status of the Participant (e.g. active, suspended or terminated) and shall be endorsed to NRoSS Sys Ad for the revocation of the digital certificate.

4.5.2.5. The NRoSS Sys Ad shall remotely revoke the digital certificate of the User/s and shall no longer require the token to be surrendered by the User to be revoked.

4.5.3. A digital certificate can only be issued or revoked but not suspended.

4.6. Operating Procedures in the Issuance and Replacement of Token

4.6.1 Issuance of token

4.6.1.1 A token shall be issued by the NRoSS Sys Ad upon the approval /endorsement of the User Enrollment Form by the NRoSS User Administrator.

4.6.1.2. The Individual Users of the Participants are required to personally receive or through the authorized representative of the Participant receive the e-token kit from NRoSS Sys Ad within the agreed scheduled between the Participant and the NRoSS Sys Ad.

4.6.1.3. A token issued to a Participant though considered owned by the Participant must be kept secure and maintained by the Participant at all times and any instance/s of damage must be immediately reported to the NRoSS User Administrator.

4.6.2 Replacement of Token

4.6.2.1. A token can only be replaced if it is lost or damaged.

4.6.2.2. A Change Request Form to replace a token and issue a new digital certificate must be submitted by the Participant to the NRoSS User Administrator for verification. NRoSS User Administrator shall then forward the Change Request Form to NRoSS SYS- AD for the creation of a new digital certificate and installation in the new token.

4.6.2.3. The Individual User shall be required to personally accept the token kit or through the authorized representative of the Participant and proceed to the NRoSS Sys Ad to receive the token kit.

## C. User Profile Management

1. The User Profile shall be managed by the following parties in the following manner:

1.1. BTr through its authorized approving officers shall be responsible for defining the User Profile to be assigned per Investor Type or Group and shall designate the following group in BTr to execute the User Profile in the NRoSS System.

1.1.1. NRoSS User Administrator – to be performed by BTr-SSRD shall be responsible for creating the Participant and Individual User details; assigning the grouping of the Participants and creating the Individual User Profile in the RoSS System based on the User Enrollment Form submitted by the Participant. It shall also create the Username and Password.
1.1.2. NRoSS Systems Administrator- to be performed by BTr-SAD shall be responsible for creating in the NRoSS System the Group User Profile that has been approved by BTr approving authorities.

1.2. Participant Access and Authentication Rights Administrator – (PA) may be a person or group of people designated by the Participant to perform the following functions:
1.2.1. Assigns the User Profile per individual users
1.2.2. Evaluates the change request of the Participant for its Users.
1.2.3. Ensures compliance of its Participant and User to the NRoSS Access Rights and Authentication Policy and pertinent rules and regulations stipulated in the Participation Agreement.
1.2.4. May also perform the function of managing the e-token (per section B.4.3.6.)

2. BTr shall define the User Profile on a group or investor type level based on the functions or roles in the primary and secondary trading and sale of government securities of the group. The User Profile of a Participant will therefore depend on the group that he was assigned to by BTr–RoSS and within a group User Profile, the Participant shall be responsible for assigning individual User Profiles.

3. The User Profile of a Participant shall remain active for as long as the Participant continues to be a Participant of the NRoSS System. In cases where the Participant is suspended or terminated upon initiation by the Participant or BTr based on grounds stipulated in the Registry Rules, the User Profile shall be managed in the following manner:

3.1 Suspension of Participant will “disable“ the participant in accessing any of its approved functionalities in the NRoSS system.

3.2. Termination of Participant will result in the “removal “of the User Profile of the Participant.

4. A Change Request Form must be submitted by the Participant for suspension and terminations initiated by them while suspension and termination

initiated by BTr shall be advised by BTr to the Participant through a written letter to be sent to the Participant and in accordance with the RoSS Operating Procedures on Suspension and Termination of Participants.

5. An Individual User Profile may be amended by the Participant by requesting (i.e. Change Request Form) for either an addition or deletion of the functionality provided it is within the approved User Profile of the Participant.