



Funding the Republic

REPUBLIKA NG PILIPINAS
KAGAWARAN NG PANANALAPI
KAWANIHAN NG INGATANG-YAMAN
(BUREAU OF THE TREASURY)
INTRAMUROS, MAYNILA 1002

MEMORANDUM

TO : ALL GSEDs, GSBs, and Other Concerned nRoSS Stakeholders

SUBJECT : nRoSS – e-Token Requirement

DATE : 09 October 2017

Providing a reliable and secure access to nRoSS System for its Participants has always been the one of the primary considerations of the Bureau of the Treasury (BTr). To address such an important requirement, we have chosen to implement a two-factor authentication (2FA) process for its access infrastructure.

The 2FA process implemented requires the use of an e-Token, which is used in tandem with the issued Username/Password of the nRoSS System. The e-Token contains a digital certificate that identifies the corresponding authorized user to access the nRoSS System. Confirmation of the e-Token access is validated via a mandatory e-Token Username/Password.


The digital certificate of the e-Token can only be generated by the BTr through its own Certificate Server. The e-Token and its inherent security features can only be obtained from the BTr.

The e-Token package (consisting of the e-Token and software license) costs Five Thousand Pesos (PHP5,000.00).

Attached is the e-Token Frequently Asked Questions (FAQs) sheet for your reference.

For further information/clarification, please contact the nRoSS Helpdesk through email address nRoSShelpdesk@treasury.gov.ph or telephone number 663-2871.

Thank you very much.


ERWIN D. STA. ANA
Officer-in-Charge &
Deputy Treasurer of the Philippines

nRoSS e-Token FREQUENTLY ASKED QUESTIONS

1. What is an e-Token?

An e-Token is a compact and portable device that allows Users of nRoSS Participants to establish secure access to the nRoSS System. Authentication is provided through the use of digital certificates.

2. What is the two-factor authentication (2FA) process for nRoSS?

Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the nRoSS User is required to undergo two separate authentication procedures using the e-Token access in conjunction with the Username/Password in the nRoSS System. Failure in any part of this authentication process means no access to the system.

3. Why is the BTr implementing a 2FA process?

Secure access to nRoSS System has always been the one of the primary considerations of the BTr. To address such an important requirement, we have chosen to implement a 2FA process for its access infrastructure.

MITM (Man in the Middle) and MITB (Man in the Browser) are examples of security attacks wherein a third party 'intercepts' or 'eavesdrops' communication content between the remote user (in this case, the nRoSS Participant) and the host server (in this case, the nRoSS System).

4. Are nRoSS Participants required to avail an e-Token?

YES. All nRoSS Participants must avail of an e-Token to be able to have initial access to the nRoSS System. The e-Token shall be used in tandem with the issued Username/Password of the nRoSS System to gain full access to nRoSS.

5. How can nRoSS Participants avail of an e-Token?

nRoSS Participants must submit a duly accomplished and approved nRoSS Participant User Enrollment Form to BTr-Scripless Securities Registration Division (SSRD). Please see documentary requirements in the BTr website.

The e-Token will only be released at the BTr offices through the MISS-System Administration Division (SAD). nRoSS Participants will have to execute an authorization letter for its personnel to receive the e-Token package for and on behalf of the institution.

6. Can Users of nRoSS Participants share an e-Token?

NO. The BTr is implementing a "One User, One e-Token" policy for security purposes. For example, if an nRoSS Participant intends to have four (4) Users, it will need to obtain 4 tokens.



7. Can the e-Token be used as a storage device?

NO. It is only used as a medium to facilitate access to the nRoSS System.

8. Can participants acquire the e-Token from another source?

NO. The e-Token can only be obtained from the BTr. Without the appropriate digital signature from the nRoSS System Certificate Server, nRoSS Participants will not be able to get the appropriate authentication requirements.

9. How much is the e-Token?

The e-Token package (consisting of the e-Token and software license) costs Five Thousand Pesos (PHP5,000.00).

10. Is the e-Token cost a one-time or recurring fee?

It is a one-time fee.

11. Do the nRoSS Participants need to renew the e-Token digital certificate?

YES. The digital certificate expires in one (1) year and shall be renewed one (1) month before the expiry date.

12. How many e-Tokens can an nRoSS Participant avail of?

Initially, up to four (4) e-Tokens. Should there be additional requirements, this will be subject to the availability and approval of the BTr.

13. What is the warranty period of the e-Token?

The e-Token has a warranty period of one (1) year. Application of warranty is subject to the approval of the BTr based on actual inspection of e-Token.

14. In case of damage or loss, what does an nRoSS Participant need to do?

a. In case of damage:

- The nRoSS Participant should immediately report the damage to the nRoSS Helpdesk.
- The nRoSS Participant should bring the damaged e-Token to the MISS-SAD for inspection.
- Once validated to be damaged, the MISS-SAD will revoke the digital certificate and prevent further access using the damaged e-Token.
- If covered by warranty, the MISS-SAD will issue a new e-Token to the nRoSS Participant. If not covered by warranty, the nRoSS Participant should avail a new e-Token subject to e-Token cost and documentary requirements.

b. In case of loss:

- The nRoSS Participant should immediately report the loss to the nROSS Helpdesk.
- The MISS-SAD will revoke the digital certificate and prevent further access using the lost e-Token.
- The nRoSS Participant should avail a new e-Token subject to e-Token cost, applicable replacement fee, if any, and documentary requirements.

SV