



# New Registry on Scripless Securities (nRoSS)

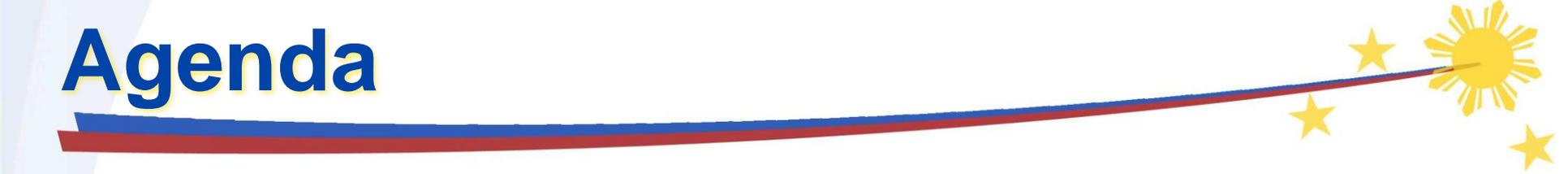
Bureau of the Treasury  
6 September, 2017



# Welcome Remarks

Bureau of the Treasury  
6 September, 2017

# Agenda



## nRoSS updates

nROSS IT related activities Overview:

Participant Access

Token Deployment

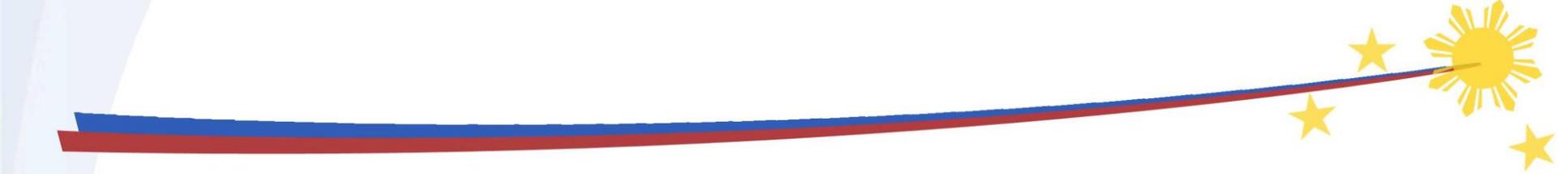
BCP – secondary access link

Parallel Run

Helpdesk

Indicative Timeline

Q & A



# nRoSS Update

# nRoSS Updates:



## nROSS Project

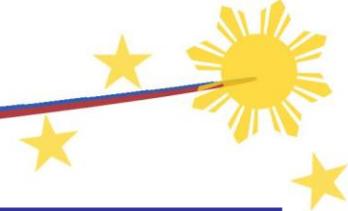
Implementation of a web-based CSD system that uses the latest technology tools and will conform to industry best practices and communication standards. The system will consolidate the auction and registry information for data mining and analytics to support policy-making activities of the BTr.

## HIGH LEVEL PROJECT SCHEDULE

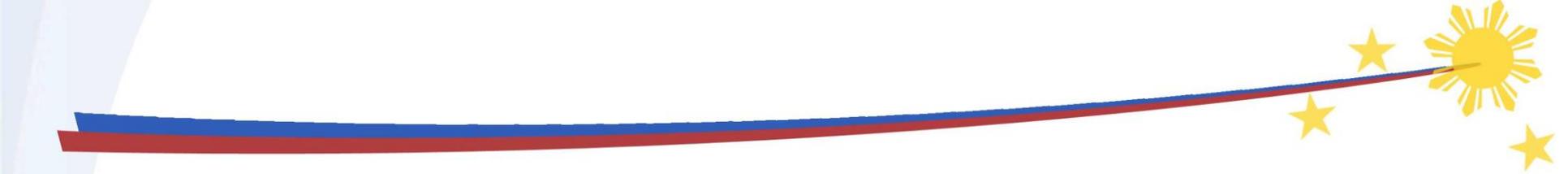
...	Milestone	Planned Start Date	Actual Start Date	Planned End	Actual End/ Revised
100%	<b>PHASE 1</b> - Inception Phase	5-Jan-16	25-Jan-16	29-Jan-16	29-Jul-16
100%	<b>Phase 2</b> - Hardware and Software Procurement, Installation	23-Feb-16	23-Feb-16	17-Jun-16	14-Jul-16
100%	<b>Phase 3A</b> - Software Customization Ver.0	5-May-16	4-Jul-16	21-Oct-16	23-Sep-16
75%	<b>Phase 4A</b> - Implementation Ver.0	3-Oct-16	3-Oct-16	<b>27-Oct-17</b>	

**Completed**

# Implementation Status



Project Activity	Status
Participant Training	- Done
Participant UAT	- Done
BTr Internal UAT	
Linkages- BSP & PDEX	nROSS can receive/send/validate settlement clearing transactions from both stakeholders (E2E)
Participant Connectivity	101/103 connected
Data Migration	-4 test pass completed. - BTr internal testing ongoing
Documentation	1. Registry rules - final review 2. Participation Agreement – final review 3. System Rules-Review ongoing 4.Participant User Manual- final review
HELPDESK	Operational
DR Site	Installation and Commissioning ongoing

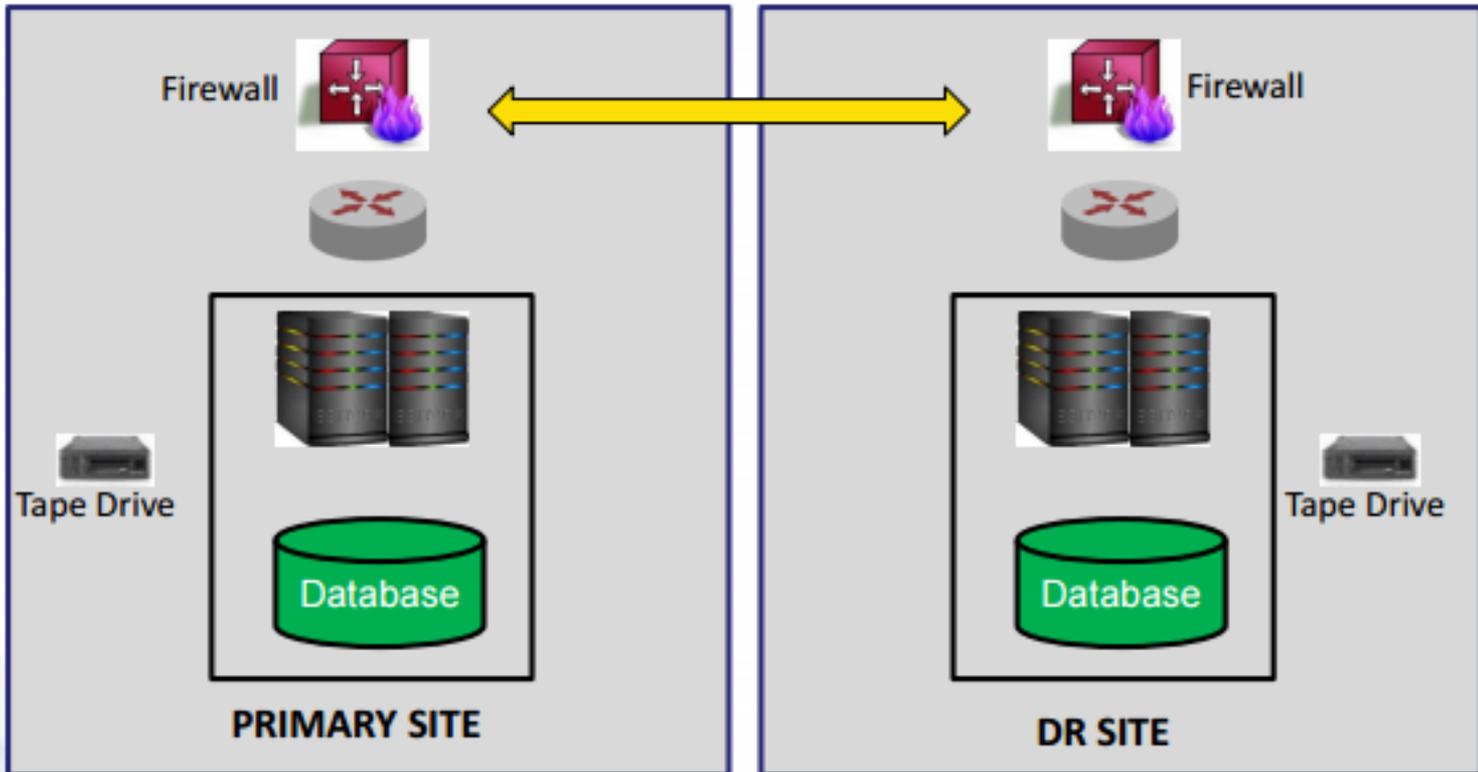
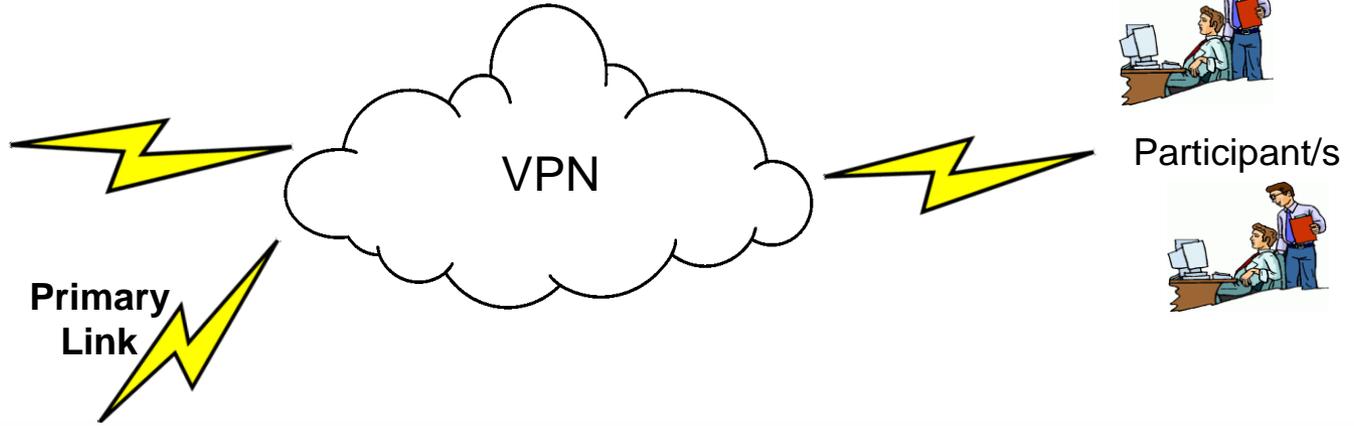


# Participant Access

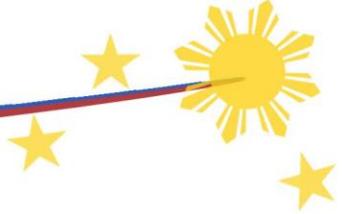
# nRoSS Connectivity

  
BSP PhilPaSS

  
PDS Gateway

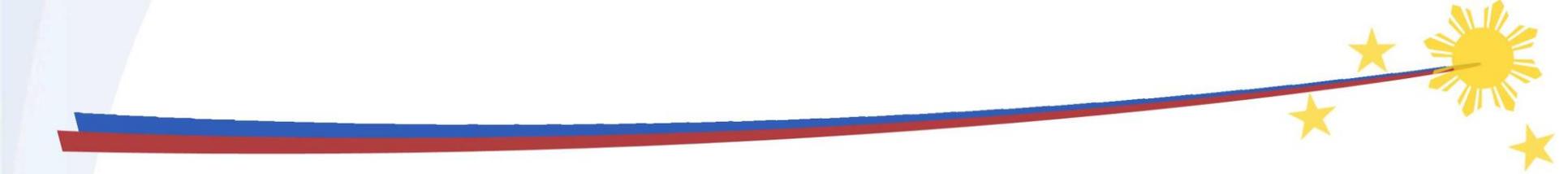


# nRoSS Connectivity



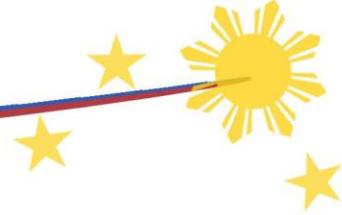
## Requirements for Participant Access to nRoSS:

- ✓ Establish internal network routing and appropriate access rights
- ✓ Allow access to USB ports
- ✓ Install client authentication software to the access device



# Token Management

# eToken Kit



**A.** eToken

**B.** CD Installer

**a.** SafeNet Client Software

**b.** How to Install SafeNet Client Software

**C.** Sealed Envelop

**a.** eToken Admin Password

**b.** eToken User Password

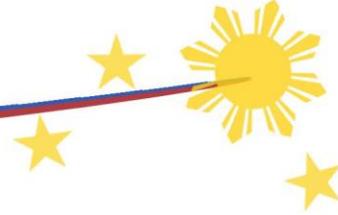
**D.** Acknowledgement Receipt Form

# What is an eToken?

- SafeNet eToken 5110 offers two-factor authentication for secure remote and network access, as well as certificate-based support for advanced security applications.

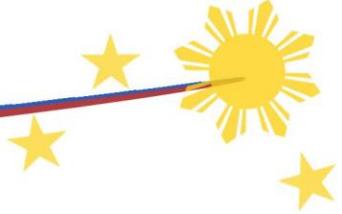


# Use of eToken



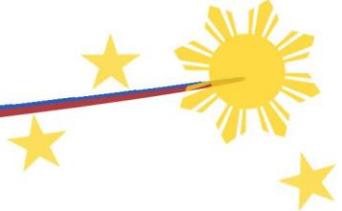
- A. The eToken is used in tandem with the issued Username/Password to authenticate Users to nRoSS and to digitally sign certain electronic messages used in the system.
- B. The SafeNet eToken 5110 or eToken for short, contains the digital certificate that will enable an authorized User to access the nRoSS infrastructure and network. The eToken shall be inserted into a designated nRoSS workstation at the Participant's site in order to log in. This eToken must not be inserted into any other device other than the designated nRoSS workstation.
- C. Access to the nRoSS system can only be obtained with the appropriate use of the eToken.
- D. The Systems Administrator of BTr-Management Information Systems Service (MISS) shall execute the configuration of the eToken for every enrolled User.
  - a. The default eToken password for Participant User and Admin will be provided by the BTr-MISS Systems Administrator.
  - b. Participant User and Admin should change the default password upon first login.

# eToken Password Policy



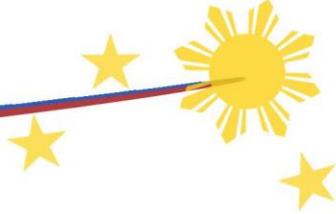
- A. Minimum Length (characters) = 8
- B. Maximum Retry Count (Users) = 5
- C. Total Complexity at least = 3
- D. Maximum Retry Count (Admin) = 5

# eToken Password Reset



- **Maximum Retry Count (Users) = 5**
  - In case of User password locked out, the Participant eToken Security Administrator can reset the User password and unlock the eToken
- **Maximum Retry Count (Admin) = 5**
  - In case of Admin password locked out, the eToken must be returned to the BTr-MISS System Administrator to initialize/reset the eToken and install a new digital certificate for reissuance

# eToken Handling



## A. Loss of eToken

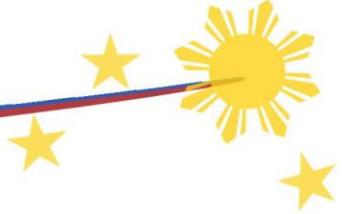
- a. Participants must immediately report any case of lost or stolen eToken to the BTr Help Desk. The BTr-MISS Systems Administrator will immediately revoke the certificate authority to prevent unauthorized access to nRoSS.
- b. A new eToken shall be issued upon request by the Participant.

Please note that if the issued eToken is lost or stolen, the Participant will shoulder the replacement cost for the issuance of a new eToken.

## B. Damage to the eToken

- a. Participants must report to BTr Help Desk any case of damaged eToken. The Participant must surrender the issued eToken to BTr-MISS office for evaluation.

# Administrative Procedures



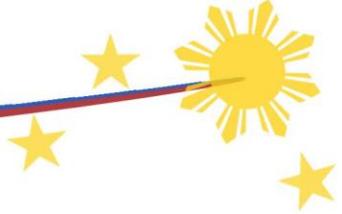
## a. 1<sup>st</sup> Issuance of eToken

- The Participant User must accomplish the nRoSS User Enrolment Form and submit to BTr for approval
- The approved form will be the basis for the creation of an nRoSS User account and issuance of a eToken kit to the Participant User. An eToken kit consists of eToken, digital certificate and eToken passwords

## b. Revocation of eToken

- An issued digital certificate may be revoked by BTr as found necessary
- A Participant can request revocation of a digital certificate to the BTr-MISS Systems Administrator thru the assigned Participant Security Administrator
- A revoked digital certificate can no longer be used to access the nRoSS system

# Administrative Procedures



## **c. Replacement of a Revoked Digital Certificate**

- For a revoked digital certificate BTr-MISS Systems Administrator will issue a new digital certificate to a Participant User
- A Participant can request issuance of a new digital certificate to BTr-MISS Systems Administrator thru their assigned Security Administrator

## **d. Renewal of a Digital Certificate**

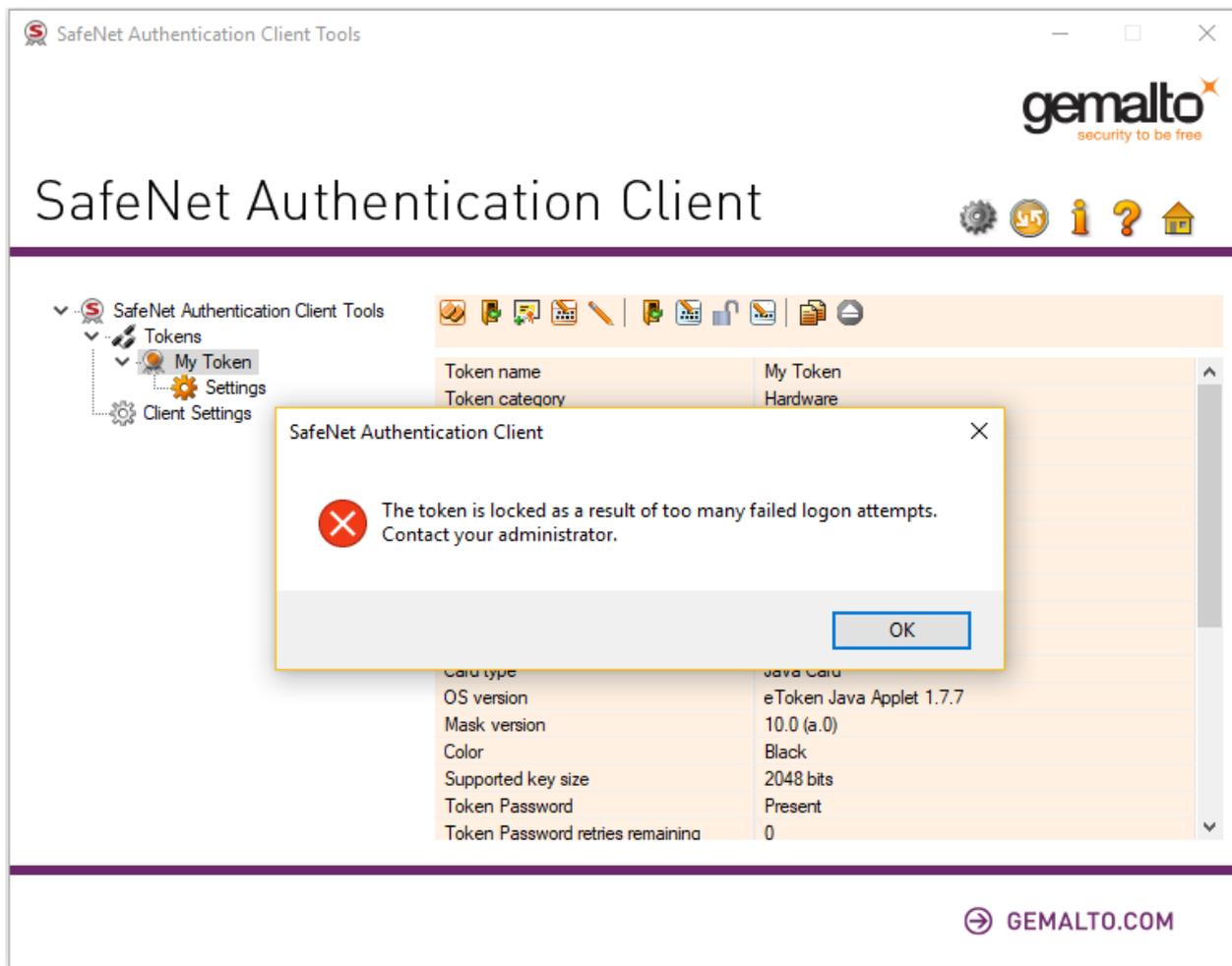
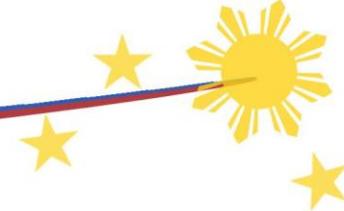
- A digital certificate is only valid for 12 months from the date of issuance to the Participant User
- A Participant must request renewal of their Users' digital certificate one month before its expiration to ensure continuity of access to nRoSS system
- A new digital certificate will be issued to the Participant User accordingly



# Reset Password of Users when Locked-out



# eToken Locked-out



The screenshot displays the SafeNet Authentication Client Tools application window. The title bar reads "SafeNet Authentication Client Tools". In the top right corner, the Gemalto logo is visible with the tagline "security to be free". Below the logo, the text "SafeNet Authentication Client" is displayed. A navigation pane on the left shows a tree view with "SafeNet Authentication Client Tools" expanded to "Tokens", which includes "My Token", "Settings", and "Client Settings". The main area shows a table of token details:

Token name	My Token
Token category	Hardware
Card type	Java Card
OS version	eToken Java Applet 1.7.7
Mask version	10.0 (a.0)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	0

An error dialog box titled "SafeNet Authentication Client" is overlaid on the table. It contains a red 'X' icon and the text: "The token is locked as a result of too many failed logon attempts. Contact your administrator." An "OK" button is located at the bottom right of the dialog box.

At the bottom right of the application window, there is a link to [GEMALTO.COM](http://GEMALTO.COM).

# Click “Log On as Administrator Button”

SafeNet Authentication Client Tools

gemalto  
security to be free

## SafeNet Authentication Client

SafeNet Authentication Client Tools

- Tokens
  - My Token
    - Settings
  - Client Settings

Token name	Log On as Administrator
Token category	Hardware
Reader name	AKS ifdh 0
Serial number	0x024f62fa
Total memory capacity	81920
Free space	32767
Hardware version	12.0
Firmware version	12.0
Card ID	024F62FA
Product name	SafeNet eToken 5110
Model	Token 12.0.0.0 12.0.12
Card type	Java Card
OS version	eToken Java Applet 1.7.7
Mask version	10.0 (a.0)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	0

GEMALTO.COM

# Input the Administrator Password

SafeNet Authentication Client Tools

gemalto  
security to be free

## SafeNet Authentication Client

Administrator Logon

SafeNet Authentication Client

gemalto  
security to be free

Enter the Token's administrator Password.

Token Name:

Administrator Password:

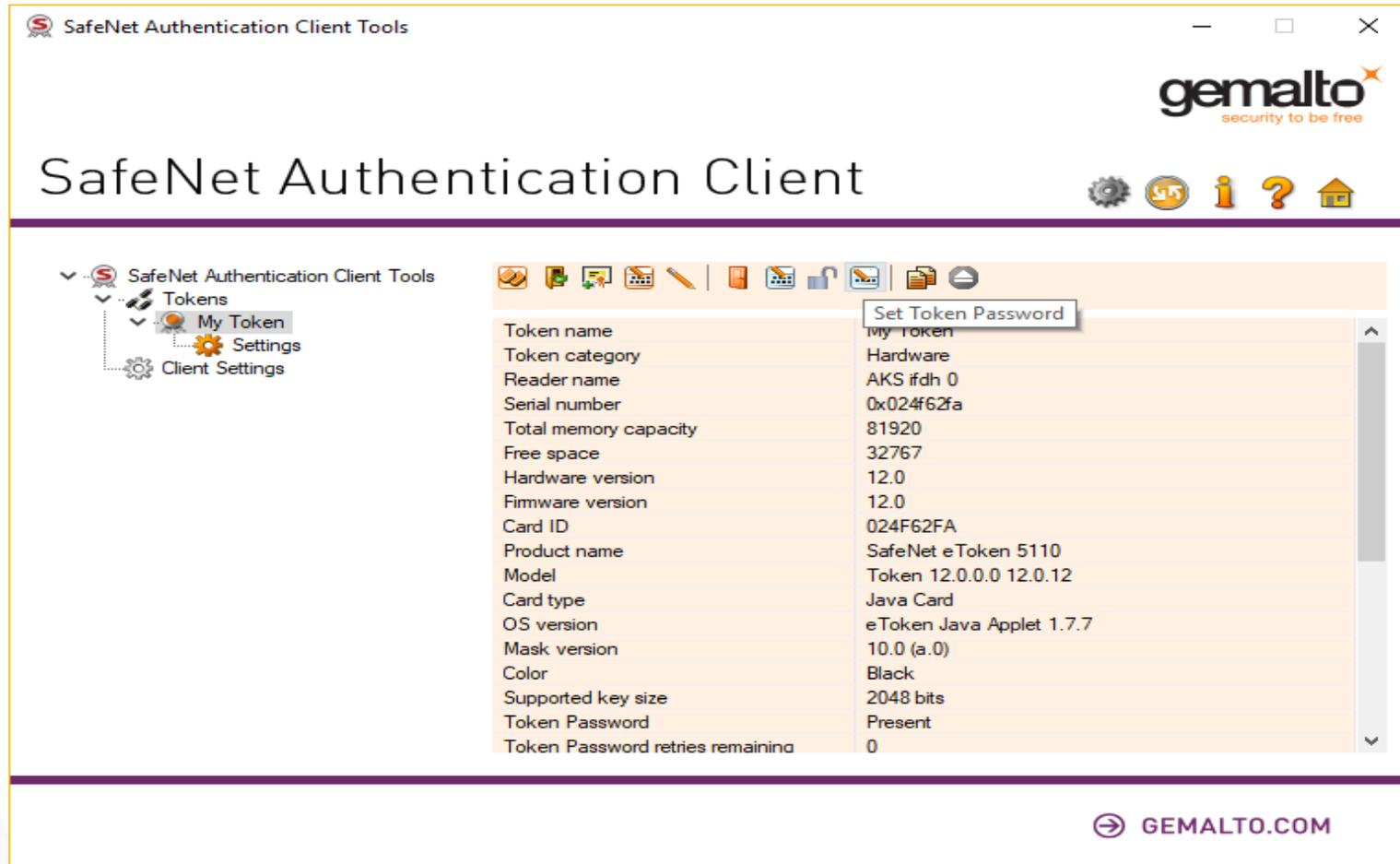
Current Language: EN

OK Cancel

Mask version	10.0 (a.0)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	0

GEMALTO.COM

# Click “Set Token Password” Button



The screenshot displays the 'SafeNet Authentication Client Tools' application window. The title bar reads 'SafeNet Authentication Client Tools' and the Gemalto logo is in the top right corner. The main window title is 'SafeNet Authentication Client'. On the left, a tree view shows 'SafeNet Authentication Client Tools' expanded to 'Tokens', then 'My Token', and finally 'Settings'. The main area shows a table of token details. A tooltip for the 'Set Token Password' button is visible over the 'Token Password' field.

Property	Value
Token name	My Token
Token category	Hardware
Reader name	AKS ifdh 0
Serial number	0x024f62fa
Total memory capacity	81920
Free space	32767
Hardware version	12.0
Firmware version	12.0
Card ID	024F62FA
Product name	SafeNet eToken 5110
Model	Token 12.0.0.0 12.0.12
Card type	Java Card
OS version	eToken Java Applet 1.7.7
Mask version	10.0 (a.0)
Color	Black
Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	0

# Input the Desired Password and Confirm

SafeNet Authentication Client Tools

gemalto  
security to be free

SafeNet Authentication Client

gemalto  
security to be free

SafeNet Auth  
Tokens  
My T  
S  
Client Set

Set Password: My Token

SafeNet Authentication Client

Token Password:

Confirm Password:   0%

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

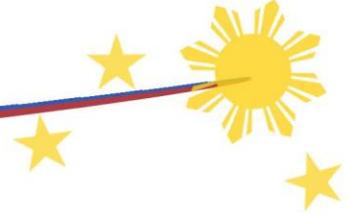
Current Language: EN

Enter a new password.

OK Cancel

Supported key size	256 bits
Token Password	Present
Token Password retries remaining	0

GEMALTO.COM



SafeNet Authentication Client Tools

gemalto  
security to be free

# SafeNet Authentication

SafeNet Authentication Client Tools

- SafeNet Authentication Client Tools
  - Tokens
    - My Token
      - Settings
        - Client Settings

Set Password: My Token

Set Password: My Token

Information Password changed successfully.

OK

Token Password: [Masked]

Confirm Password: [Masked] 100%

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

Current Language: EN

OK Cancel

Supported key size	2048 bits
Token Password	Present
Token Password retries remaining	15

GEMALTO.COM



# Changing the Password of the User



# Click “Change Token Password” Button

The screenshot displays the 'SafeNet Authentication Client Tools' application window. The title bar reads 'SafeNet Authentication Client Tools' and includes standard window controls. The main header area features the 'gemalto' logo with the tagline 'security to be free' and a navigation bar with icons for settings, status, help, and home. The main content area is titled 'SafeNet Authentication Client' and contains a 'My Token' section on the left. On the right, a vertical list of buttons is shown: 'Rename Token', 'Change Token Password' (highlighted with a blue border), 'Unlock Token', 'Delete Token Content', 'View Token Info', and 'Disconnect SafeNet eToken Virtual'. The bottom right corner of the window contains the 'GEMALTO.COM' logo.

# Input the Current and Desired Password

SafeNet Authentication Client Tools

gemalto  
security to be free

SafeNet

My Tok

Change Password: My Token

SafeNet Authentication Client

gemalto  
security to be free

Current Token Password:

New Token Password:

Confirm Password:  100%

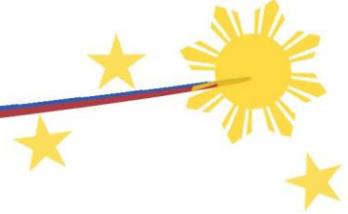
The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

Current Language: EN

OK Cancel

GEMALTO.COM



SafeNet Authentication Client Tools

gemalto  
security to be free

# SafeNet

My Token

gemalto  
security to be free

Change Password: My Token

SafeNet Authentication Client

Current Token Password: [password field]

New Token Password:

Confirm Password:

The new password must

A secure password has a minimum of 8 characters, including upper-case letters, lower-case letters, numerals, and special characters.

Current Language: EN

OK Cancel

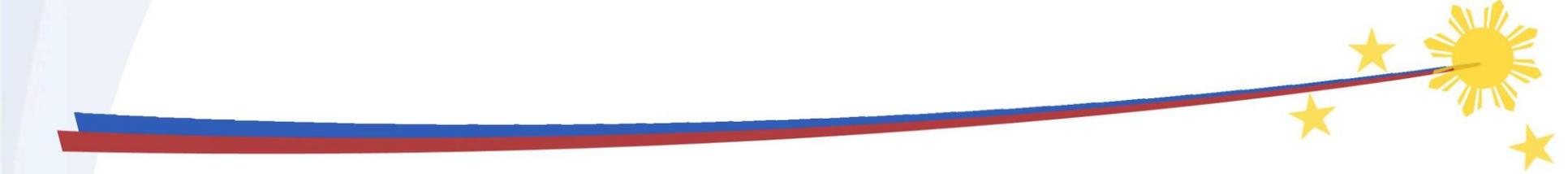
Change Password: My Token

**i** Password changed successfully.

OK

100%

GEMALTO.COM

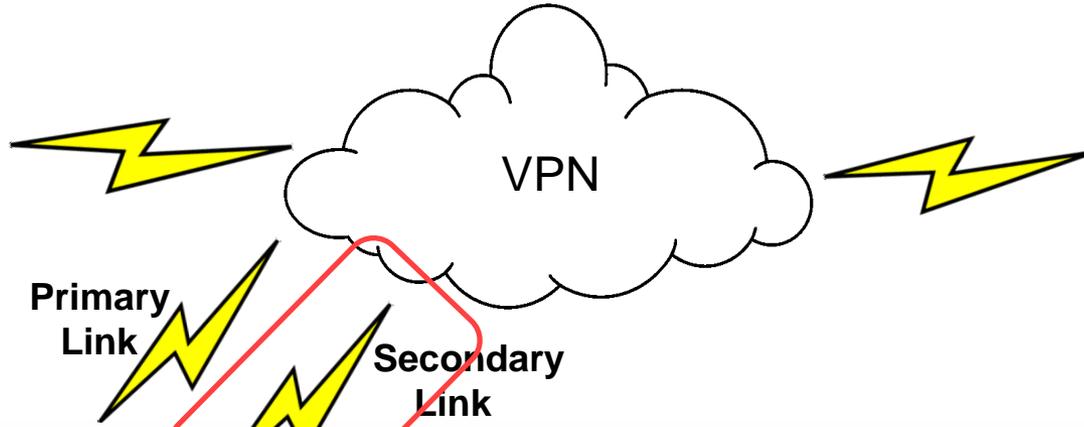


# **BCP – Secondary link**

# nRoSS secondary link:

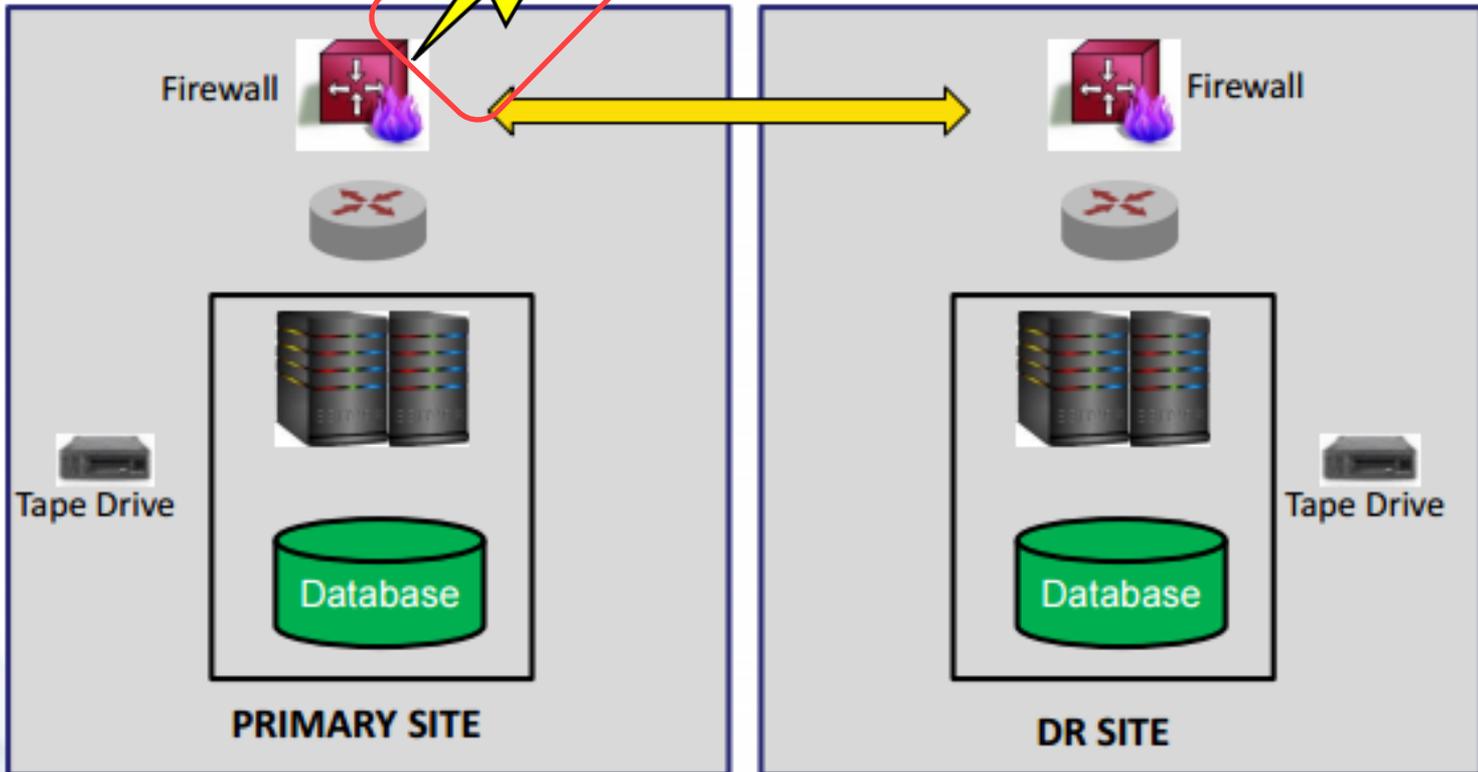
  
BSP PhilPaSS

  
PDS Gateway

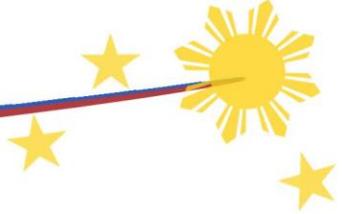


Primary Link

Secondary Link



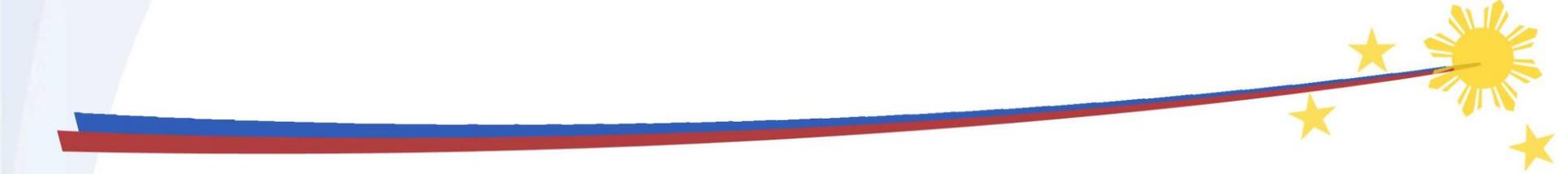
# nRoSS Secondary Link Activation



- New VPN form enrolment (**Deadline for submission: September 19, 2017**)
- BTR-Participant configuration to existing firewall linked to nRoSS
- Schedule link testing

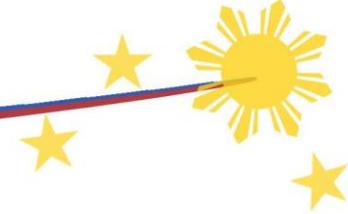
**Secondary Link Activation:**

**September 30, 2017**



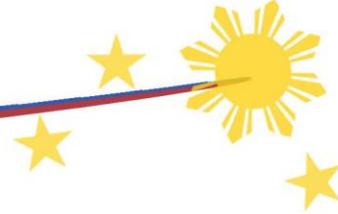
# Helpdesk

# HELPDESK Contacts



Item	Details
Email Address	nrosshelpdesk@treasury.gov.ph
Telephone Number	663-2871
Availability	8AM-5PM (Business Days)

# HELPDESK Procedure



## Participant

## 1<sup>st</sup> Level of Support

## 2<sup>nd</sup> Level of Support



Participant  
Calls/Emails  
nRoSS  
HelpDesk

Initial  
troubleshooting  
procedure.

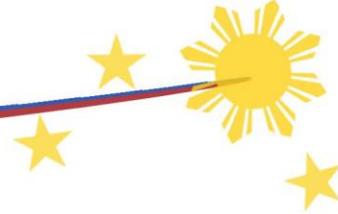
BTr nRoSS Specialists  
(IT, AUCTION, RoSS)

## 3<sup>rd</sup> Level of Support



Every reported issue is given a HelpDesk Ticket number. Once resolved, the ticket will be closed.

# Email Reporting

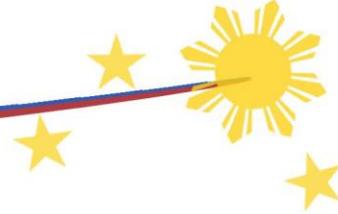


For concerns/issues reported to nRoSS HelpDesk via the Email Address, please ensure to include the ff:

1. **Participant Entity Name**
2. **nRoSS Username used to access nRoSS**
  - a. Full Name of the Participant/Username
  - b. Role of the Username – ex: Dealer, Broker, Custodian, Trust, Depository, Regulator, SGA
3. **Complete Details of the Issue/Concern** (sample questions like)
  - a. What were you trying to do?
  - b. Which screen/module were you trying to access?
4. **If available, please indicate the “Error Message” displayed by the system**
5. **It is always preferable to include “screenshots” of the issue/concern for faster investigation and resolution**



# Sample Email



Email Subject: nRoSS UAT Issue: Cannot bid  
To: nrosshelpdesk@treasury.gov.ph

Dear, nRoSS HelpDesk.

Good day.

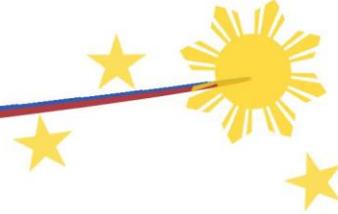


This is to request assistance of the following nRoSS concern/issue.

Details as follows:

1. Participant Name: BPI
2. nRoSS Username used to access nRoSS: juandelacruz@bpi.com
  - a. Juan Dela Cruz
  - b. Role: Dealer
3. Concern/Issue:
  - a. Cannot bid in auction 3DAY TBILLS
  - b. Module: Competitive auction
4. Error Message encountered : “Error 123: Cannot bid”
5. Please see attached screenshots of the error encountered

# Call Reporting

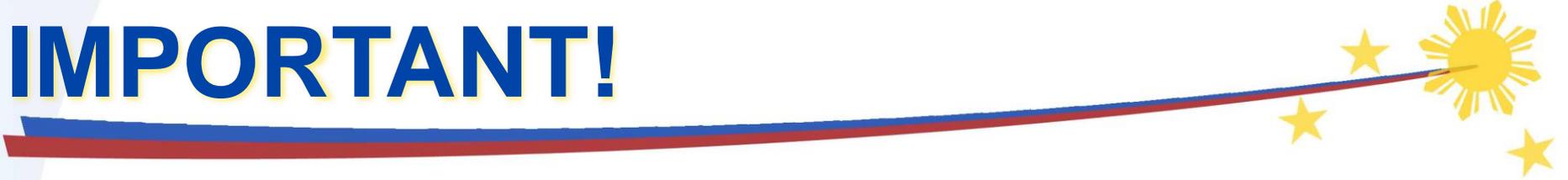


For concerns/issues reported to nRoSS HelpDesk via the Telephone number, please ensure to include the ff:

- 1. Participant Entity Name**
- 2. nRoSS Username used to access nRoSS**
  - a. Full Name of the Participant/Username
  - b. Role of the Username – ex: Dealer, Broker, Custodian, Trust, Depository, Regulator, SGA
- 3. Complete Details of the Issue/Concern** (sample questions like)
  - a. What were you trying to do?
  - b. Which screen/module were you trying to access?
- 4. If available, please indicate the “Error Message” displayed by the system**



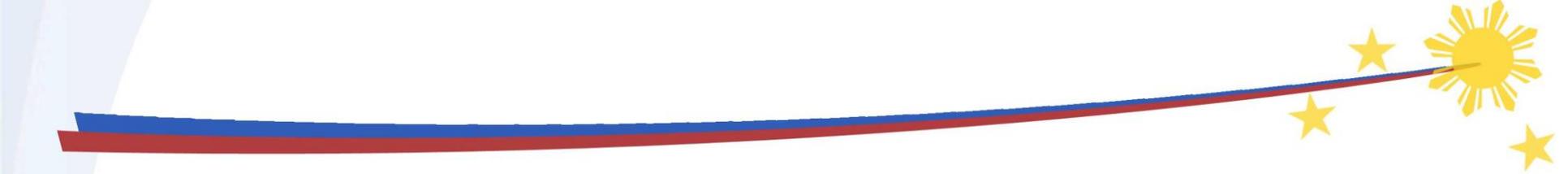
# IMPORTANT!



Please report any testing  
issue/concern you encounter

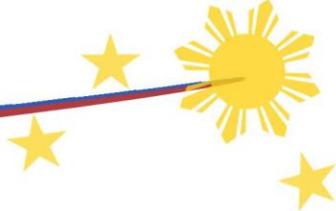
**THE SOONEST**

(preferably **as and when it happens**  
so we can investigate and resolve  
accordingly)



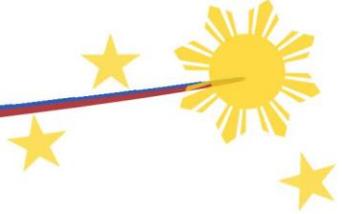
# Parallel Run

# Auction Parallel Run



- nROSS will run parallel with ADAPS (starting Sept. 25 T-Bill auction)
  - Participant GSEDs will enter bids in both ADAPS and nROSS
  - nROSS team will compare results from both systems
- Requirements for auction Parallel Run:
  - ✓ Participant Access to nRoSS
  - ✓ eToken deployment (2 per GSED)
  - ✓ User enrolment forms

# Secondary Market Testing



- Market-wide testing for secondary market
  - Participants are expected to enter test transactions through the test environment of the trading platform during a specified trading window.
  - BTR and PDS to coordinate activity