



MANAGEMENT INFORMATION SYSTEMS SERVICE
National Registry of Scripless Securities (NRoSS)
VPN CONNECTIVITY REGISTRATION FORM

Name of Participating Entity (PE)/Institution:		Date of Request:
Complete Address: <i>(Please indicate ZIP Code)</i>		Contact No:
A. VPN Configuration Requirements		
Please see Annex A		
B. Participant IT Network Support Information		
Name of IT Personnel: (Last Name, First Name, MI)	Email Address	Contact No./Mobile No.
TERMS and CONDITIONS		
<i>The requested VPN access to BTr facility is provided for the exclusive use of Participating Entities (PE)/Institutions to allow access to the National Registry of Scripless Securities (NRoSS) testing and production environment. The request must be accomplished by the authorized system user that is approved and signed by the Head of the Institution/Authorized Signatory.</i>		
<i>The requesting PE/Institution must abide or conform to the BTr technical requirements. The PE/Institution shall be responsible for any hardware/software upgrades required to support the VPN connectivity. Support shall be provided for BTr-specific VPN connectivity only. BTr must be informed for any changes in the VPN configuration five (5) days in advance to avoid disruption of the services.</i>		
<i>BTr may revoke, block or permanently disallow the use of this service without prior notice due to reasons that may compromise BTr internal ICT security. Any breach or compromise in NRoSS Services shall be immediately relayed to the BTr-MIS Service through the NRoSS Customer Contact no. at 663-2266 or at email address: btrsystad@treasury.gov.ph</i>		
I. Agreement: I, hereby agree to the above terms and conditions. I also agree to keep confidential all information regarding the VPN. I will not disclose password information and/or copy the VPN settings onto unauthorized users/computers. Propagating BTr VPN configuration is considered a security breach and is ground for the termination of the account. <div><div>_____</div><div>Authorized User (Signature over Printed Name)</div></div> <div><div>_____</div><div>Date</div></div>	II. Approved by: <div><div>_____</div><div>Head of Institution/Authorized Signatory (Signature over Printed Name)</div></div> <div><div>_____</div><div>Date</div></div>	
(To be accomplished by BTr)		
III. Recommending Approval: <div><div>_____</div><div>Authorized MISS IT Officer (Signature over Printed Name)</div></div> <div><div>_____</div><div>Date</div></div>	IV. Approved by: <div><div>_____</div><div>Director, MIS Service (Signature over Printed Name)</div></div> <div><div>_____</div><div>Date</div></div>	
Processed by: <div><div>_____</div><div>Authorized MISS IT Officer (Signature over Printed Name)</div></div> <div><div>_____</div><div>Date</div></div>	Remarks:	

ANNEX A: VPN Configuration Form

VPN Configuration Form

FOR PR/DR ENVIRONMENT

Site 1: BTrnRoSS		Site 2: - Participant Site
------------------	--	----------------------------

VPN Information			VPN Information	
Supplier:	Fortinet		Supplier:	
Type:			Type:	
Model:			Model:	
OS:			OS:	
Public IP Peer address:	103.159.253. 249 (primary) 203.160.172.18 (secondary) 103.233.35.20 (DR)		Public IP Peer address:	
IKE Proposal Parameters (Phase 1)			IKE Proposal Parameters (Phase 1)	
Proposal Name:	BTr-NRoSS		Proposal Name:	
Authentication Mode:	Pre-shared Key		Authentication Mode:	
Preshared Key:	To be emailed separately		Preshared Key:	
Authentication Algorithm:	SHA-512		Authentication Algorithm:	
Encryption Algorithm:	AES256		Encryption Algorithm:	
Diffie-Hellman Group:	DH Group 21		Diffie-Hellman Group:	
Lifetime Measurement:			Lifetime Measurement:	
Keylife:	86400		Keylife:	
Dead Peer Detection:	Enabled		Dead Peer Detection:	
IPSEC Parameters (Phase 2)			IPSEC Parameters (Phase 2)	
Authentication Algorithm:	SHA-512		Authentication Algorithm:	
Encryption Algorithm:	AES256		Encryption Algorithm:	
Diffie-Hellman Group:	DH Group 21		Diffie-Hellman Group:	
Encapsulation Mode:	IPSec		Encapsulation Mode:	
Perfect Forward Secrecy:	Enabled		Perfect Forward Secrecy:	
Lifetime Measurement:			Lifetime Measurement:	
Keylife:	43200		Keylife:	
Replay Detection:	Enabled		Replay Detection:	
VPN Tunnel Access List Information			VPN Tunnel Access List Information	
Network Address /Netmask:	172.31.20.106/32 (PR) 172.31.20.103/32(TEST) 172.31.70.106/32 (DR)		Network Address Translated IP:	
Firewall Security Rules			Firewall Security Rules	
Hostname	Address(:Port)		Hostname	Address(:Port)
	7036			
	icmp/ping			
	443			
			Intended number of users	
			Site to Site	Client to Site
Contact Information				
BTr – Systems Administration Division	8663-2266			
Note: Items in red font are required parameters. To test connectivity, please access IP(web browser) https://172.31.20.106:7036/csd for primary and secondary lines, for TEST environment and https://172.31.70.106:7036/csd for DR line.				