For Email Address Verification Procedures

Non Project – Ministry of Foreign Affairs VPN/Secure Email (MFA-VPN)

Description: Ambassadors from Ministry of Foreign Affairs uses VPN access and Secure Email for all diplomatic relations and communications. Ministry of Foreign affairs uses Netrust **Managed** digital certificates for **Signing, Encryption, Confidentiality & Authentication** for its diplomatic endeavours.

### CHECKLIST

Appointed site managers manage user applications. Site managers will provide the following for new applications.

* Email request indicating Bulk Application (to be printed out)
* Encrypted & Signed Bulk Input request form

#### CERTIFICATE GENERATION

For each user indicated in the bulk input do the following

1. Click the New User Icon. Enter the First Name and Last Name as stated in the bulk input form.
2. Enter the Serial Number in the following format

SG-[Identity No]:E:[Running Number]

ie.. SG-S1234567A:E:0

The running number typical starts at 0 for the first cert. Increment it by one for each additional cert issuance. NOTE : Applicants must hold ICA approved ID documents only (ie.. NRIC, FIN & EP only).

1. Enter the users required email address in the “Email” field.
2. In the “Add to:” select the “Ministry of Foreign Affairs”
3. In the “Certificate Info” tab, Select “Enterprise” under Category and “Corporate Netrust Corporate Enterprise Certificates” under Type.
4. Use default values for “General” and “Key Update Options” tabs. Click ok when done. Encrypt and email the generated Authorisation Code and Reference No to the site manager who made the request.



For Code Signing Subscriber Verification Procedures

Non-Project – Server (Enterprise/Web)

Description: Server certs are issued as **Managed or Unmanaged** digital certificates for **Confidentiality,** **Encryption & Authentication**.

### CHECKLIST

* Netrust Corporate Server Application Form (NAM)
* Letter of Authorisation (LoA) for the representative to collect the cert
* Photocopy of the ***Company RCB/ROC from ACRA*** as proof of rights (PoR)
* Original & Photocopy (front & back) of identification document (ID). Acceptable document includes NRIC, FIN, EP or Passport.
* Certificate Server Request (CSR Optional) – For customer hosting own private key. Refer to **F. Generating a Web Server cert with CSR**

#### CERTIFICATE GENERATION (ENTERPRISE)

1. Create the Searchbase Server/“Company Name” (as stated in PoR). For sole proprietors, use the Searchbase Server instead.

Refer to **E. How to Create/Add a new Server Searchbase (ou=)**

1. Click the New User Icon. Select the type Web Server under the naming tab. Enter the Name for the server as stated in Netrust Corporate Server Application Form.
2. In the “Add to:” select the Searchbase determined in Step 1.
3. In the “Certificate Info” tab, Select “Enterprise” under Category and “Corporate Netrust Server Enterprise Certificates” under Type.
4. Use default values for “General” and “Key Update Options” tabs. Click ok when done. Generate the cert as type V2 into a Safenet token.

#### CERTIFICATE GENERATION (WEB)

1. Create the Searchbase Server/“Company Name” (as stated in PoR). For sole proprietors, use the Searchbase Server instead.

Refer to **E. How to Create/Add a new Server Searchbase (ou=)**

1. Click the New User Icon. Select the type Web Server under the naming tab. Enter the Name for the server as stated in Netrust Corporate Server Application Form.
2. In the “Add to:” select the Searchbase determined in Step 1.
3. In the “Certificate Info” tab, Select “Web” under Category and “Web Server Netrust Netserver Server Web Certificates” under Type.
4. Use default values for “General” tabs. Click ok when done. Generate the cert using NetrustConnector. (https://netrustconnector.netrust.net/alternate.htm)

EnterpriseWeb

For audits

Auditor: Tay Ghim Hui (Associate Security Consultant)

Email: tay.ghimhui@e-cop.net

Date : 25 April 2010