Bugzilla ID: 632292
Bugzilla Summary: Add Netrust root certificate

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	Netrust Pte Ltd
Website URL	http://www.netrust.net
Organizational type	private corporation
Primark Market / Customer Base	Netrust is a private corporation in Singapore, which provides individuals, business and government organizations with a complete online identification and security infrastructure to enable secure electronic transactions. Besides certificate provisioning, Netrust delivers high quality professional services including security consulting, PKI deployment and custom application development. Netrust was awarded by the International Civil Aviation Organization (ICAO) to setup and operate the global Public Key Directory (PKD).
Impact to Mozilla Users	Relying parties while web browsing
CA Contact Information	CA Email Alias: noc@netrust.net CA Phone Number: 621212378 Title / Department: System Engineer/OPS Team

Technical information about each root certificate

Certificate Name	Netrust CA1
Certificate Issuer Field	OU = Netrust CA1; O = Netrust Certificate Authority 1; C = SG
Certificate Summary	Root cert used to secure government sites and company using CA ROOT cert. Ministry of Foreign Affairs VPN/Secure Email: 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 endeavors. Server (Enterprise/Web): Server certs are issued as Managed or Unmanaged digital certificates for Confidentiality, Encryption & Authentication.
Root Cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=512868
SHA1 Fingerprint	55:C8:6F:74:14:AC:8B:DD:68:14:F4:D8:6A:F1:5F:37:10:E1:04:D0
Valid From	2001-03-29
Valid To	2021-03-29
Certificate Version	3
Certificate Signature Algorithm	SHA-1
Signing key parameters	2048

Test Website URL (SSL)	Provide a URL to a website whose SSL cert chains up to this root. Note that this can be a test site.
CRL URL	http://netrustconnector.netrust.net/netrust.crl CPS 4.4.9.1: Netrust updates and publishes the Certificate Revocation List (CRL) every forty-eight hours.
OCSP URL	none
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV
EV Policy OID(s)	Not requesting EV

CA Hierarchy information for each root certificate

CA Hierarchy	The "Netrust CA1" root signs end-entity certificates directly. It does not have any subordinate CAs. Issuing end-entity certs directly from the root is not as secure as using an offline root and issuing certificates using a subordinate CA. Why does your root directly sign end-entity certs? What actions are taken to mitigate the risk? Is it possible for you to modify your practices such that the root cert is offline and only signs intermediate CAs which sign end-entity certs?
Externally Operated SubCAs	None
Cross-Signing	None

Verification Policies and Practices

Policy Documentation	Language(s) that the documents are in: English CPS: https://www.netrust.net/docs/ourpractices/cps.pdf On https://www.netrust.net/ourpractices.php in the Certificate Policies section it says: "Netrust issues multiple classes of certificates to support different certificate user communities. Each class of certificates is governed by a CP that differentiates the use of the certificates for different application purposes and/or by different certificate user communities. The CP(s) include:" Which of the certificates in the list chain up to this root?
Audits	Audit Type: ISO27001/27002:2005 Auditor: Tay Ghim Hui (Associate Security Consultant) Email: tay.ghimhui@e-cop.net Auditor Website:http://www.e-cop.net/ The audit type must be one of the criteria listed in #9 of http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html The auditor must meet the requirements of #10 and #11 of http://www.mozilla.org/projects/security/certs/policy/InclusionPolicy.html We do not expect that the full, detailed audit report be provided. However, the auditor must provide a statement about what was audited, the criteria that was use, and a summary of the findings.

SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide English translations of the relevant sections of publicly available documentation regarding all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Be sure to provide the urls and section numbers of the original text.
EV SSL Verification Procedures	Not applicable; not requesting EV treatment.
Organization Verification Procedures	CPS section 3.1.8 and 3.1.9
Email Address Verification Procedures	CPS 3.1.9.2: For e-mail validation, identification and authentication of the individual will be done by checking and verifying that the e-mail address of the Subscriber does in fact exist. This is not sufficient; we need more info about how this verification is done. If you are requesting to enable the Email Trust Bit, then provide English translations of the relevant sections of publicly available documentation regarding all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Be sure to provide the urls and section numbers of the original text. 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). 3. Enter the users required email address in the “Email” field. 4. In the “Add to:” select the “Ministry of Foreign Affairs” 5. In the “Certificate Info” tab, Select “Enterprise” under Category and “Corporate Netrust Corporate Enterprise Certificates” under Type. 6. 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.

Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide English translations of the relevant sections of publicly available documentation regarding all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices Be sure to provide the urls and section numbers of the original text. 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=) 2. 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. 3. In the "Add to:" select the Searchbase determined in Step 1. 4. In the "Certificate Info" tab, Select "Enterprise" under Category and "Corporate Netrust Server Enterprise Certificates" under Type. 5. 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=) 2. 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. 3. In the "Add to:" select the Searchbase determined in Step 1. 4. In the "Certificate Info" tab, Select "Web" under Category and "Web Server Netrust Netserver Server Web Certificates" under Type. 5. Use default values for "General" tabs. Click ok when done. Generate the cert using NetrustConnector. (https://netrustconnector.netrust.net/alternate.htm)

Please review and respond to Mozilla's list of Potentially Problematic Practices.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	No
Wildcard DV SSL certificates	No
Email Address Prefixes for DV Certs	No
Delegation of Domain / Email validation to third parties	Yes there is delegation of domain and email but there is no validation to third parties What does this mean?
Issuing end entity certificates directly from roots	Yes See questions above.
Allowing external entities to operate subordinate CAs	No
Distributing generated private keys in PKCS#12 files	No
Certificates referencing hostnames or private IP addresses	Yes How are the potential problems mitigated?
Issuing SSL Certificates for Internal Domains	Yes How are the potential problems mitigated?
OCSP Responses signed by a certificate under a different root	No
CRL with critical CIDP Extension	Yes Needs to be changed – CRLs must load into Firefox without error.
Generic names for CAs	No
Lack of Communication With End Users	No