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	Indicate whether the CA is operated by a private or public corporation, government agency, international organization, academic institution or consortium, NGO, etc. Note that in some cases the CA may be of a hybrid type, e.g., a corporation established by the government. For government CAs, the type of government should be noted, e.g., national, regional/state/provincial, or municipal.
Primark Market / Customer Base	Which types of customers does the CA serve? Are there particular vertical market segments in which it operates? Does the CA focus its activities on a particular country or other geographic region?
Impact to Mozilla Users	Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.
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	Provide a summary about this root certificate, it's purpose, and the types of certificates that are issued under it.
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. If you are requesting EV treatment, then the SSL cert must have the EV Policy OID.
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	If you are requesting to enable EV, then OCSP must be provided. OCSP URI in the AIA of end-entity certs Maximum expiration time of OCSP responses Testing results a) Browsing to test website with OCSP enforced in Firefox browser b) If requesting EV: https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	OV and EV
EV Policy OID(s)	2.16.840.1.114028.10.1.2

CA Hierarchy information for each root certificate

CA Hierarchy	Provide a description, list, and/or diagram of all sub-CAs chaining up to this root. Identify which subCAs are internally-operated and which are externally operated.
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
Audits	Audit Type: Auditor: Auditor Website: URL to Audit Report and Management's Assertions: Date of completion of last audit:
SSL Verification Procedures	If you are requesting to enable the Websites Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
EV SSL Verification Procedures	If you are requesting EV treatment, then please provide links to the documents describing your EV policies and practices.
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 (In English and in publicly available documentation) all the information requested in #4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices
Code Signing Subscriber Verification Procedures	If you are requesting to enable the Code Signing Trust Bit, then provide (In English and in publicly available documentation) all the information requested in #5 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices The CP/CPS must include specific information about Code Signing certificates.

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	
Wildcard DV SSL certificates	
Email Address Prefixes for DV Certs	
Delegation of Domain / Email validation to third parties	
Issuing end entity certificates directly from roots	
Allowing external entities to operate subordinate CAs	
Distributing generated private keys in PKCS#12 files	
Certificates referencing hostnames or private IP addresses	
Issuing SSL Certificates for Internal Domains	
OCSP Responses signed by a certificate under a different root	
CRL with critical CIDP Extension	
Generic names for CAs	
Lack of Communication With End Users	