Bugzilla ID: 577665
Bugzilla Summary: Add Trustis FPS Root CA Certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	Trustis
Website URL	http://www.trustis.com/
Organizational type	Public, Commercial CA
Primary market / customer base	Trustis is a commercial CA operating primarily in the UK and Europe.
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. Note the Mozilla CA certificate policy: • Section 1: We will determine which CA certificates are included in software products distributed through mozilla.org, based on the benefits and risks of such inclusion to typical users of those products. • Section 6: We require that all CAs whose certificates are distributed with our software product ... provide some service relevant to typical users of our software products
CA Contact Information	CA Email Alias: info@trustis.com An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: +44 (0) 1865 736780 Title / Department: PKI

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	Data
Certificate Name	Trustis FPS Root CA

	CN <Not Part Of Certificate>
	OU = Trustis FPS Root CA
	O = Trustis Limited
	C = GB

Cert summary / comments	
Root Cert URL	http://www.trustis.com/roots/fps/certs/fpsroot.crt
SHA-1 fingerprint	3B:C0:38:0B:33:C3:F6:A6:0C:86:15:22:93:D9:DF:F5:4B:81:C0:04
Valid from	2003-12-23
Valid to	2024-01-21
Cert Version	3
Modulus length	2048
Test Website	For testing purposes, please 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://www.trustis.com/pki/fps/crl/fpsder.crl CP section 4.4.9: the Issuing Authority shall ensure that publication of valid certificate status information is scheduled at least every 24 hours.
OCSP Responder URL	None
CA Hierarchy	Trustis FPS CA Hierarchy: https://bugzilla.mozilla.org/attachment.cgi?id=268357 Is this diagram still current? Trustis FPS Offline CA -> Online Issuing CAs -> End-entity certs
Externally operated subCAs	The Trustis FPS Enterprise Authority is the subCA used for issuing general SSL certificates. The Trustis DTP Issuing Authority does not issue SSL certificates. The Trustis Healthcare Issuing Authority issues SSL certificates to UK NHS facilities. All subCAs issuing certificates must do so in accordance with the UK Gov't Authentication Framework - Level 2. This is required for all certificates from all of the FPS subCAs be they individual or SSL. In the case of SSL, this means certs issued are of level 3 or higher. Domains are validated but a number of other criteria relating to the organization and the individual representing the organization must also be satisfied. Please see https://wiki.mozilla.org/CA:SubordinateCA_checklist and provide the requested information.
Cross-Signing	None, as per diagram
Requested Trust Bits	Website Email
SSL Validation Type	OV The organisation authentication includes verification of the organisation, the person representing the organisation, and the authority of that person to apply for the certificate. The PDS then makes the statement that 'Additional data, including declared domain names and other data .... are subject to independent verification'.

If DV – email addresses used for verification	If SSL certificates are issued with only DV verification, then please provide the list of acceptable email addresses that are used for verification. Please see: https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership and https://wiki.mozilla.org/CA:Problematic_Practices#Email_Address_Prefixes_for_DV_Certs The list that the CA uses must either match or be a subset of the list in the Problematic_Practices wiki page.
EV policy OID(s)	Not applying for EV at this time.
CP/CPS	All Documents are in English Trustis Document Repository: http://www.trustis.com/pki/fpsia/ Trustis FPS Certificate Policy: http://www.trustis.com/pki/fpsia/policy/T-FPS-CP-V1-04.pdf This document specifies the minimum requirements to be observed in the issuance, management, usage and reliance-on certificates. Trustis FPS Issuing Authority PKI Disclosure Statement: http://www.trustis.com/pki/fpsia/policy/disclosure.htm Subscriber Agreement: http://www.trustis.com/pki/fpsia/policy/subscriber-agreement.htm
AUDIT	Audit Type: WebTrust CA Auditor: KPMG Audit Report and Management's Assertions: http://cert.webtrust.org/ViewSeal?id=1060 (2010.05.30) Trustis is also ISO 27001 accredited and has been tScheme approved (https://www.tscheme.org/directory/trustis/index.html).
Organization Identity Verification	CP Section 3: Identification and Authentication CP Section 3.1.8: The Issuing Authority in section 2 of PKI Disclosure Statement or other community-wide accessible document shall define the mechanisms to be used that support the level of confidence required in the identity asserted by a digital certificate issued under this Certificate Policy. We rely on publicly available documentation and audits of those documented processes to ascertain that the CA takes reasonable measures to confirm the identity and authority of the individual and/or organization of the certificate subscriber. Please list the documents and section or page numbers where this information can be found.
Domain Name Ownership / Control	Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership We rely on publicly available documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Please list the corresponding document(s) and section or page numbers containing this information.

Email Address Ownership / Control	Please see https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control We rely on publicly available documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met. Section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; Please list the corresponding document(s) and section or page numbers containing this information.
Identity of Code Signing Subscriber	Not applicable. Not requesting Code Signing trust bit.
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information and pointers to the relevant documentation. • Long-lived DV certificates ○ • Wildcard DV SSL certificates ○ • Email Address Prefixes for DV SSL Certs ○ • Delegation of Domain / Email validation to third parties ○ Yes. Registration Authorities are used as per section 1.3.2.3 of the CP. ○ We'll need further info about the controls (policies, audits) that are place on these third parties. • Issuing end entity certificates directly from roots ○ No. Root signs intermediate CAs only. • Allowing external entities to operate unconstrained subordinate CAs ○ Yes. Required to follow practices, and be audited annually. ○ Please provide the links and section numbers of the documentation describing the controls (policies, audits) that are placed on external entities operating sub-CAs. • Distributing generated private keys in PKCS#12 files ○ Yes, Trustis provides the option of generating the private key. (section 4.1 of CP) • Certificates referencing hostnames or private IP addresses ○ • Issuing SSL Certificates for Internal Domains

	○ • OCSP Responses signed by a certificate under a different root ○ OCSP not provided • CRL with critical CIDP Extension ○ • Generic names for CAs ○ O an OU include Trustis.