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	▪ Government and private sector users of web services related to the UK NHS ▪ Ministry of Defense users of web-based payroll services ▪ Government and commercial users of web services related to the UK Emissions Registry (Carbon-credit trading) ▪ Government and private sector users of e-services related to UK Local Councils ▪ Public and private sector users of e-services related to HM Government ▪ Commercial entities leveraging B2B secure email services
CA Contact Information	CA Email Alias: info@trustis.com 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
Issued By	CN <Not Part Of Certificate> O = Trustis Limited OU = Trustis FPS Root CA
Cert summary / comments	This root signs internally-operated subordinate CAs that sign end-entity certs.
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	https://www.trustis.com/
CRL URL	ARL: http://www.trustis.com/pki/fps/crl/fpsder.crl CRL for end-entity certs: http://www.trustis.com/pki/trustis-ssl/crl/ee.crl (NextUpdate: 24 hours) CP section 4.4.9: CRL for end-entity certs 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 The "Trustis FPS Root CA" root is offline. It signs internally-operated Issuing CAs that sign end-entity certs. - 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 Government 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.
Externally operated subCAs	All of the subCA's are hosted, managed and operated by Trustis Limited.
Cross-Signing	None, as per diagram.
Requested Trust Bits	Website Email
SSL Validation Type	OV
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 Minimum Enrolment Requirements: http://www.trustis.com/pki/fpsia/policy/T-0104-002-ATL-013-Trustis-FPS-Minimum-Enrolment-Requirements-V3_0.pdf Trustis FPS Certificate Policy: http://www.trustis.com/pki/fpsia/policy/T-FPS-CP-V1-04.pdf 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 UK Government Authentication Framework (GAF) – HMG Minimum Requirements for Verification: Individuals: http://www.cabinetoffice.gov.uk/media/252559/regindividualsv2.pdf Organizations: http://www.cabinetoffice.gov.uk/media/252565/registra_orgs_v2.pdf
AUDIT	Audit Type: WebTrust CA Auditor: KPMG Audit Report and Management's Assertions: https://cert.webtrust.org/ViewSeal?id=1120 (2010.12.31) Trustis is also ISO 27001 accredited and tScheme approved (https://www.tscheme.org/directory/trustis/index.html).

Organization Identity Verification	Trustis FPS Minimum Enrolment Requirements: http://www.trustis.com/pki/fpsia/policy/T-0104-002-ATL-013-Trustis-FPS-Minimum-Enrolment-Requirements-V3_0.pdf See this document for details about verification of individual and organization. There are two tables showing the required evidence and the validity criteria for individual and organization. "Trustis FPS issues certificates to a number of levels of assurance and authentication. In all cases certificates issued shall fulfil the Standards of HMG Assurance Framework, specifically: · HMG Minimum Requirements for the Verification of the Identity of Individuals V2 · HMG Minimum Requirements for the Verification of the Identity of Organisations V2 at level two." … "Note that a formal documented existing relationship with the RA may be used in lieu of / with other evidence if the RA already has strong confidence in the identity of the registrant organisation. Underlying identification checks must have been previously performed and it is essential to ensure that information used is up-to-date." … "In each case and for each certificate applicant, the Registrar may: · Take further steps to confirm the identity and eligibility of the intended subscriber. This may include the use of independent confirmation with other parties. · Approve the certificate request if the Registrar is sufficiently satisfied of the identity and eligibility of the intended certificate holder (Subscriber). … · Defer the certificate request, pending further investigation of the identity and eligibility of the intended subscriber · Reject the request"
Domain Name Ownership / Control	Trustis FPS Minimum Enrolment Requirements: http://www.trustis.com/pki/fpsia/policy/T-0104-002-ATL-013-Trustis-FPS-Minimum-Enrolment-Requirements-V3_0.pdf "The registration data for the domain is collected from approved and/or third party public sources (WHOIS) and corroborated against the information verified as part of the individual or organisation registration submitted in the application. Where third party or public evidence does not provide corroboration of ownership of a domain, or an organisation or individual controls a domain not registered with it. Certified written evidence of ownership/control must be provided. This is verified and/or corroborated with the registered owner of the domain." Comment #23: All certificate requests require manual checking and RA Operators have been advised of the domains to be aware of. Each day all certificates issued in the last 24 hours are checked against the list of domains.
Email Address Ownership / Control	Trustis FPS Minimum Enrolment Requirements: http://www.trustis.com/pki/fpsia/policy/T-0104-002-ATL-013-Trustis-FPS-Minimum-Enrolment-Requirements-V3_0.pdf "Back contact using the declared email address and or third party corroboration is undertaken as part of the enrolment process."

	"Certificates are not issued on the basis of email address only. Applicants must fulfil all identity verification requirements AND prove ownership of the email address to be identified in the certificate. Identity, or Active in the Community Documents as specified in these requirements that contain the email address"
Identity of Code Signing Subscriber	Not applicable. Not requesting Code Signing trust bit.
Multi-factor Authentication	Comment #23: We can confirm that all accounts capable of directly causing certificate issuance require two factor authentication.
Network Security	Comment #23: We have audited our PKI and no sign of intrusion or compromise is evident. The audit also reviewed the network security controls and found no potential issues.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• Long-lived DV certificates
	  ○ SSL certs are OV
	• Wildcard DV SSL certificates
	  ○ SSL certs are OV
	• Email Address Prefixes for DV SSL Certs
	  ○ SSL certs are OV
	• Delegation of Domain / Email validation to third parties
	  ○ **Yes. Registration Authorities are used as per section 1.3.2.3 of the CP.**
	  ○ From Trustis: Registration Authorities (RAs) are permitted to conduct registrations for a limited, defined and controlled number and type of end-entities. The RAs have to operate in compliance with the Certificate Policy (CP) and Certification Practice Statement (CPS) and also our declared authentication levels for the Trustis FPS services, which are set at HMG Authentication Framework Level 2 or higher. These are controlled under our CP, a variety of internal and third party audits and the specific contractual relationship.
	• Issuing end entity certificates directly from roots
	  ○ No. Root signs intermediate CAs only.
	• Allowing external entities to operate unconstrained subordinate CAs
	  ○ All sub-CAs are internally operated.
	• Distributing generated private keys in PKCS#12 files
	  ○ Yes, Trustis provides the option of generating the private key. (section 4.1 of CP)
	  ○ From Trustis: End-entity key generation and delivery is only permitted on an exceptional basis and providing it does not impact the integrity of the service. When such activities are undertaken the requirements specified within the CP and Subscriber Agreement must be followed. Our records indicate that, to date for Trustis FPS, this activity has never been undertaken.
	• Certificates referencing hostnames or private IP addresses
	  ○ Trustis does not issue certificates referencing internal hostnames and/or private IP addresses.

	• Issuing SSL Certificates for Internal Domains
	  ○ Trustis does not issue SSL certificates for internal domains.
	• OCSP Responses signed by a certificate under a different root
	  ○ OCSP not provided
	• CRL with critical CIDP Extension
	  ○ CRLs import into Firefox without error.
	• Generic names for CAs
	  ○ O an OU include Trustis.