Print this page

Mozilla - CA Program

Case Information

Case Number	00000104	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Google Trust Services (GTS)	**Request Status**	Initial Request Received

Additional Case Information

Subject	Google Trust Services (GTS) Root Certificate	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1325532

General information about CA's associated organization

CA Email Alias 1	contact@pki.goog		
CA Email Alias 2			
Company Website	https://pki.goog	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)	N/A	**Verified?**	Not Applicable
Geographic Focus	Global	**Verified?**	Verified
Primary Market / Customer Base	GTS issues server authentication, client authentication, email (both signing and encrypting), and code signing certs to the general public.	**Verified?**	Verified
Impact to Mozilla Users		**Verified?**	Need Response From CA

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	1) Publicly Available CP and CPS: 2) CA Hierarchy: 3) Audit Criteria: 4) Document Handling of IDNs in CP/CPS: 5) Revocation of Compromised Certificates: 6) Verifying Domain Name Ownership: 7) Verifying Email Address Control: 8) Verifying Identity of Code Signing Certificate Subscriber:	**Verified?**	Need Response From CA

9) DNS names go in SAN:
10) Domain owned by a Natural Person:
11) OCSP:
12) Network Security Controls:

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	1) Long-lived DV certificates: 2) Wildcard DV SSL certificates: 3) Email Address Prefixes for DV Certs: 4) Delegation of Domain / Email validation to third parties: 5) Issuing end entity certificates directly from roots: 6) Allowing external entities to operate subordinate CAs: 7) Distributing generated private keys in PKCS#12 files: 8) Certificates referencing hostnames or private IP addresses: 9) Issuing SSL Certificates for Internal Domains: 10) OCSP Responses signed by a certificate under a different root: 11) SHA-1 Certificates: 12) Generic names for CAs: 13) Lack of Communication With End Users: 14) Backdating the notBefore date:	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	GTS Root R1	**Root Case No**	R00000144
Request Status	Initial Request Received	**Case Number**	00000104

Certificate Data

Certificate Issuer Common Name	GTS Root R1
O From Issuer Field	Google Trust Services LLC
OU From Issuer Field	
Valid From	2016 Jun 22
Valid To	2036 Jun 22
Certificate Serial Number	6e47a9c54b470c0dec33d089b91cf4e1
Subject	CN=GTS Root R1, OU=null, O=Google Trust Services LLC, C=US
Signature Hash Algorithm	sha384WithRSAEncryption
Public Key Algorithm	RSA 4096 bits

SHA-1 Fingerprint	E1:C9:50:E6:EF:22:F8:4C:56:45:72:8B:92:20:60:D7:D5:A7:A3:E8
SHA-256 Fingerprint	2A:57:54:71:E3:13:40:BC:21:58:1C:BD:2C:F1:3E:15:84:63:20:3E:CE:94:BC:F9:D3:CC:19:6B:F0:9A:54:72
Certificate Fingerprint	1A:B8:8F:E2:C4:8A:31:F5:43:5F:3E:E3:A2:2F:35:43:79:CC:1E:28:BD:EB:B3:D1:E7:02:ED:48:17:44:15:89
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	GTS Root R1 is a Root CA with an RSA key with a 4096 bit long modulus. It will be used to issue a variety of certificate types via intermediates specific for each certificate type, there will be one intermediate, “GTS X1”	**Verified?**	Verified
Root Certificate Download URL	https://pki.goog/gtsr1.crt	**Verified?**	Verified
CRL URL(s)	http://crl.pki.goog/gtsr1/gtsr1.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.pki.goog/gstr1	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	No EV request	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://good.r1demo.pki.goog	**Verified?**	Verified
Test Website - Expired	https://expired.r1demo.pki.goog		
Test Website - Revoked	https://revoked.r1demo.pki.goog		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: Browse to https://crt.sh/ and enter the SHA-1 Fingerprint for the root certificate. Then click on the 'Search' button. Then click on the 'Run cablint' link. All errors must be resolved/fixed.	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed.	**Verified?**	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language	English		
CP	https://pki.goog/GTS-CP-1.0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pki.goog/GTS-CPS-1.0.pdf	**Verified?**	Verified
Other Relevant Documents	N/A	**Verified?**	Verified
Auditor Name	Ernst and Young USA	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	Web Trust for CAs: https://cert.webtrust.org/ViewSeal?id=2124 Web Trust BRs: https://cert.webtrust.org/ViewSeal?id=2125	**Verified?**	Need Clarification From CA
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 ofhttps://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response

			From CA
Standard Audit Type	WebTrust	**Verified?**	Need Clarification From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type	WebTrust	**Verified?**	Need Clarification From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	No EV request	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	No EV request	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Root Case Record # 2

Root Case Information

Root Certificate Name	GTS Root R2	**Root Case No**	R00000145
Request Status	Initial Request Received	**Case Number**	00000104

Certificate Data

Certificate Issuer Common Name	GTS Root R2
O From Issuer Field	Google Trust Services LLC
OU From Issuer Field	
Valid From	2016 Jun 22
Valid To	2036 Jun 22
Certificate Serial Number	6e47a9c65ab3e720c5309a3f6852f26f
Subject	CN=GTS Root R2, OU=null, O=Google Trust Services LLC, C=US
Signature Hash Algorithm	sha384WithRSAEncryption
Public Key Algorithm	RSA 4096 bits
SHA-1 Fingerprint	D2:73:96:2A:2A:5E:39:9F:73:3F:E1:C7:1E:64:3F:03:38:34:FC:4D
SHA-256 Fingerprint	C4:5D:7B:B0:8E:6D:67:E6:2E:42:35:11:0B:56:4E:5F:78:FD:92:EF:05:8C:84:0A:EA:4E:64:55:D7:58:5C:60
Certificate Fingerprint	0E:5C:2C:B5:0C:8C:C2:7F:F4:E1:C7:28:05:07:3A:67:1B:BC:51:76:3B:83:10:73:5C:6F:EC:3B:DE:93:F9:EB
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	GTS Root R3 is a Root CA with an ECDSA key using secp384r1. It will be used to issue a variety of certificate types via intermediates specific for each certificate type, there will be one intermediate, “GTS X3”	**Verified?**	Verified
Root Certificate Download URL	https://pki.goog/gtsr2.crt	**Verified?**	Verified
CRL URL(s)	https://crl.pki.goog/gtsR2/gtsr2.crl	**Verified?**	Verified
OCSP URL(s)	https://ocsp.pki.goog/gstr2	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	No EV request	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://good.r2demo.pki.goog	**Verified?**	Verified
Test Website - Expired	https://expired.r2demo.pki.goog		
Test Website - Revoked	https://revoked.r2demo.pki.goog		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: Browse to https://crt.sh/ and enter the SHA-1 Fingerprint for the root certificate. Then click on the 'Search' button. Then click on the 'Run cablint' link. All errors must be resolved/fixed.	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed.	**Verified?**	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language	English		
CP	https://pki.goog/GTS-CP-1.0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pki.goog/GTS-CPS-1.0.pdf	**Verified?**	Verified
Other Relevant Documents	N/A	**Verified?**	Not Applicable
Auditor Name	Ernst and Young USA	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	Web Trust for CAs: https://cert.webtrust.org/ViewSeal?id=2124 Web Trust BRs: https://cert.webtrust.org/ViewSeal?id=2125	**Verified?**	Need Clarification From CA
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 ofhttps://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Need Clarification From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type	WebTrust	**Verified?**	Need Clarification From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	No EV request	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable	**Verified?**	Need Response From CA

	description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership		
EV SSL Verification Procedures	No EV request	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Root Case Record # 3

Root Case Information

Root Certificate Name	GTS Root R3	**Root Case No**	R00000146
Request Status	Initial Request Received	**Case Number**	00000104

Certificate Data

Certificate Issuer Common Name	GTS Root R3
O From Issuer Field	Google Trust Services LLC
OU From Issuer Field	
Valid From	2016 Jun 22
Valid To	2036 Jun 22
Certificate Serial Number	6e47a9c76ca9732440890f0355dd8d1d
Subject	CN=GTS Root R3, OU=null, O=Google Trust Services LLC, C=US
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	30:D4:24:6F:07:FF:DB:91:89:8A:0B:E9:49:66:11:EB:8C:5E:46:E5
SHA-256 Fingerprint	15:D5:B8:77:46:19:EA:7D:54:CE:1C:A6:D0:B0:C4:03:E0:37:A9:17:F1:31:E8:A0:4E:1E:6B:7A:71:BA:BC:E5
Certificate Fingerprint	57:D8:8B:41:7F:B7:8B:E3:05:55:8C:96:4B:36:63:66:1E:FF:AF:2E:B6:82:9D:1D:31:7D:92:00:1B:F6:6C:79
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	GTS Root R2 is a Root CA with an RSA key with a 4096 bit long modulus. It will be used to issue a variety of certificate types via intermediates specific for each certificate type, there will be one intermediate, "GTS X2".	Verified?	Verified
Root Certificate Download URL	https://pki.goog/gtsr3.crt	Verified?	Verified
CRL URL(s)	https://crl.pki.goog/gtsr3/gtsr3.crl	Verified?	Verified
OCSP URL(s)	https://ocsp.pki.goog/gstr3	Verified?	Verified
Trust Bits	Code; Email; Websites	Verified?	Verified
SSL Validation Type	DV; OV	Verified?	Verified
EV Policy OID(s)	No EV request	Verified?	Not Applicable
Root Stores Included In	Microsoft	Verified?	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	Verified?	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://good.r3demo.pki.goog	Verified?	Verified
Test Website - Expired	https://expired.r3demo.pki.goog		
Test Website - Revoked	https://revoked.r3demo.pki.goog		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	Verified?	Need Response From CA
CA/Browser Forum Lint Test	NEED: Browse to https://crt.sh/ and enter the SHA-1 Fingerprint for the root certificate. Then click on the 'Search' button. Then click on the 'Run cablint' link. All errors must be resolved/fixed.	Verified?	Need Response From CA
Test Website Lint Test	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed.	Verified?	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	Verified?	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue	Verified?	Need Response From CA

	different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements		
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language	English		
CP	https://pki.goog/GTS-CP-1.0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pki.goog/GTS-CPS-1.0.pdf	**Verified?**	Verified
Other Relevant Documents	N/A	**Verified?**	Not Applicable
Auditor Name	Ernst and Young USA	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	Web Trust for CAs: https://cert.webtrust.org/ViewSeal?id=2124 Web Trust BRs: https://cert.webtrust.org/ViewSeal?id=2125	**Verified?**	Need Clarification From CA
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 ofhttps://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Need Clarification From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA

BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type	WebTrust	**Verified?**	Need Clarification From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	No EV request	**Verified?**	Need Response From CA
EV Audit Type		**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA
EV SSL Verification Procedures	No EV request	**Verified?**	Need Response From CA
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA

Root Case Record # 4

Root Case Information

Root Certificate Name	GTS Root R4	**Root Case No**	R00000147

Request Status	Initial Request Received	**Case Number**	00000104

Certificate Data

Certificate Issuer Common Name	GTS Root R4
O From Issuer Field	Google Trust Services LLC
OU From Issuer Field	
Valid From	2016 Jun 22
Valid To	2036 Jun 22
Certificate Serial Number	6e47a9c88b94b6e8bb3b2ad8a2b2c199
Subject	CN=GTS Root R4, OU=null, O=Google Trust Services LLC, C=US
Signature Hash Algorithm	ecdsaWithSHA384
Public Key Algorithm	EC secp384r1
SHA-1 Fingerprint	2A:1D:60:27:D9:4A:B1:0A:1C:4D:91:5C:CD:33:A0:CB:3E:2D:54:CB
SHA-256 Fingerprint	71:CC:A5:39:1F:9E:79:4B:04:80:25:30:B3:63:E1:21:DA:8A:30:43:BB:26:66:2F:EA:4D:CA:7F:C9:51:A4:BD
Certificate Fingerprint	20:57:9A:7F:A6:01:79:75:8D:7F:59:14:C1:ED:CD:A9:77:B8:FD:70:D1:CA:28:A1:61:3F:D5:FD:37:EA:45:91
Certificate Version	3

Technical Information about Root Certificate

Certificate Summary	GTS Root R4 is a Root CA with an ECDSA key using secp384r1. It will be used to issue a variety of certificate types via intermediates specific for each certificate type, there will be one intermediate, “GTS X4”	**Verified?**	Verified
Root Certificate Download URL	https://pki.goog/gtsr4.crt	**Verified?**	Verified
CRL URL(s)	https://crl.pki.goog/gtsR4/gtsr4.crl	**Verified?**	Verified
OCSP URL(s)	https://ocsp.pki.goog/gstr4	**Verified?**	Verified
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV	**Verified?**	Verified
EV Policy OID(s)	No EV request	**Verified?**	Verified
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	NEED: Mozilla has the ability to name constrain root certs; e.g. to *.gov or *.mil. CAs should consider if such constraints may be applied to their root certs. https://dxr.mozilla.org/mozilla-central/source/security/nss/lib/certdb/genname.c#1551	**Verified?**	Need Response From CA

Test Websites or Example Cert

Test Website - Valid	https://good.r4demo.pki.goog	**Verified?**	Verified
Test Website - Expired	https://expired.r4demo.pki.goog		
Test Website -	https://revoked.r4demo.pki.goog		

Revoked	
Example Cert	
Test Notes	

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED: Test with http://certificate.revocationcheck.com/ make sure there aren't any errors.	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: Browse to https://crt.sh/ and enter the SHA-1 Fingerprint for the root certificate. Then click on the 'Search' button. Then click on the 'Run cablint' link. All errors must be resolved/fixed.	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: Browse to https://cert-checker.allizom.org/ and enter the test website and click on the 'Browse' button to provide the PEM file for the root certificate. Then click on 'run certlint'. All errors must be resolved/fixed.	**Verified?**	Need Response From CA
EV Tested	NEED: If EV treatment is being requested, then provide successful output from EV Testing as described here https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version	**Verified?**	Need Response From CA

CA Hierarchy Information

CA Hierarchy	NEED: A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate. - List and/or describe all of the subordinate CAs that are signed by this root. - Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on. - It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do not require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED: - If this root has any subordinate CA certificates that are operated by external third parties, then provide the information listed in the Subordinate CA Checklist,https://wiki.mozilla.org/CA:SubordinateCA_checklist - If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.	**Verified?**	Need Response From CA
Cross Signing	NEED: - List all other root certificates for which this root certificate has issued cross-signing certificates. - List all other root certificates that have issued cross-signing certificates for this root certificate. - If any such cross-signing relationships exist, it is important to note whether the cross-signing CAs' certificates are already included in the Mozilla root store or not.	**Verified?**	Need Response From CA
Technical Constraint on 3rd party Issuer	NEED: CP/CPS documentation describing the technical and contractual controls over any 3rd party who may issue certs in this CA Hierarchy. This includes external RAs as well as External subCAs. References: - section 7.1.5 of version 1.3 of the CA/Browser Forum's Baseline Requirements - https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/inclusion/ - https://wiki.mozilla.org/CA:CertificatePolicyV2.1#Frequently_Asked_Questions	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy	NEED: Languages that the CP/CPS and other documents are provided in.	**Verified?**	Need

Documentation			Response From CA
CA Document Repository		**Verified?**	Need Response From CA
CP Doc Language	English		
CP	https://pki.goog/GTS-CP-1.0.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://pki.goog/GTS-CPS-1.0.pdf	**Verified?**	Verified
Other Relevant Documents	N/A	**Verified?**	Not Applicable
Auditor Name	Ernst and Young USA	**Verified?**	Verified
Auditor Website	http://www.ey.com/	**Verified?**	Verified
Auditor Qualifications	Web Trust for CAs: https://cert.webtrust.org/ViewSeal?id=2124 Web Trust BRs: https://cert.webtrust.org/ViewSeal?id=2125	**Verified?**	Need Response From CA
Standard Audit	NEED: for all root inclusion/change requests. Reference section 2 ofhttps://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Standard Audit Type	WebTrust	**Verified?**	Need Clarification From CA
Standard Audit Statement Date		**Verified?**	Need Response From CA
BR Audit	NEED: If requesting Websites trust bit, then also need a BR audit as described here: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type	WebTrust	**Verified?**	Need Clarification From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	No EV request	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Need Response From CA
EV Audit Statement Date		**Verified?**	Need Response From CA
BR Commitment to Comply	NEED section in the CP/CPS that has the commitment to comply with the BRs as described in section 2.2 of version 1.3 of the CA/Browser Forum's Baseline Requirements.	**Verified?**	Need Response From CA
SSL Verification Procedures	NEED: if Websites trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the domain name to be included in the SSL/TLS cert. As per section 3 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs It is not sufficient to simply reference the section of the CA/Browser Forum's Baseline Requirements (BR) that lists the ways in which the CA may confirm that the certificate subscriber owns/controls the domain name to be included in the certificate. The CA's CP/CPS must specify which of those options the CA uses, and must include a reasonable description of the ways the CA can verify that the certificate subscriber owns/controls the domain name(s) to be included in the certificate. https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Domain_Name_Ownership	**Verified?**	Need Response From CA

EV SSL Verification Procedures	No EV request	**Verified?**	Not Applicable
Organization Verification Procedures	NEED: CP/CPS sections that describe identity and organization verification procedures for cert issuance.	**Verified?**	Need Response From CA
Email Address Verification Procedures	NEED if Email trust bit requested... Sections of CP/CPS that sufficiently describe the verification steps that are taken to confirm the ownership/control of the email address to be included in the cert. As per section 4 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices https://wiki.mozilla.org/CA:Recommended_Practices#Verifying_Email_Address_Control	**Verified?**	Need Response From CA
Code Signing Subscriber Verification Pro	Mozilla is no longer accepting requests to enable the Code Signing trust bit.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED CA response (and corresponding CP/CPS sections/text) to section 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED CA response (and corresponding CP/CPS sections/text) to section 7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA