This Document summarizes the information gathered and verified for the following 3 CA inclusion requests.
Bugzilla ID: 430694
Bugzilla Summary: Enable GTE CyberTrust Global Root for EV Extended Validation SSL
Bugzilla ID: 430698
Bugzilla Summary: Enable Baltimore CyberTrust Root for EV Extended Validation SSL
Bugzilla ID: 430700
Bugzilla Summary: Add Cybertrust Global Root, plus enable EV SSL support

Mozilla CA certificate policy: http://www.mozilla.org/projects/security/certs/policy/

General Information	**Data**
CA Name	Verizon Business, a division of Verizon Communications. (Formerly known as Cybertrust, Betrusted, Baltimore Technologies and GTE CyberTrust)
Website URL	http://www.verizonbusiness.com/us/products/security/identity/ http://cybertrust.omniroot.com/repository.cfm
Organizational type	Public corporation
Primary market / customer base	Verizon Business Security Solutions Powered by Cybertrust operates a commercial certificate authority service for businesses and governments internationally.

CA Info

Info Needed	**Data – Bug #430694**	**Data – Bug #430698**	**Data – Bug #430700**
Root Name	GTE CyberTrust Global Root	Baltimore CyberTrust Root	Cybertrust Global Root
Description	This request is to EV-enable a root that is already available in Firefox. This root has been embedded in PKI enabled products since its creation in 1998. This is presently our mainstream root, issuing our standard validation SSL server certificates, user authentication and secure email certificates, and code signing certificates. Currently the Websites and Email trust bits are enabled in the GTE CyberTrust Global Root built-in object. This request is to also enable the Code Signing trust bit.	This request is to EV-enable a root that is already available in Firefox. This root will supersede the GTE CyberTrust Global Root. Currently only the Websites trust bit is enabled in the Baltimore CyberTrust Root built-in object. This request is to also enable the Email and Code Signing trust bits.	This is a new root to be added to the Mozilla NSS database, and to be EV-enabled. This root was created to provide a service to customers desiring a root based outside the United States. It was created in December 2006 to immediately fix a limitation in Windows XP and IE 7 where existing roots could not be marked with EV ability. Relying on the GTE CyberTrust Global Root for ubiquity through cross-certification, this is our main root for issuance of EV SSL certificates.
Root CA certificate URL	Available in Firefox	Available in Firefox	http://cacert.omniroot.com/ct_root_ss.crt

SHA-1 fingerprint.	97:81:79:50:d8:1c:96:70:cc:34:d8:09:cf:79:44:31:36:7e:f4:74	d4:de:20:d0:5e:66:fc:53:fe:1a:50:88:2c:78:db:28:52:ca:e4:74	5f:43:e5:b1:bf:f8:78:8c:ac:1c:c7:ca:4a:9a:c6:22:2b:cc:34:c6
Valid from	1998-08-12	2000-05-12	2006-12-15
Valid to	2018-08-13	2025-05-12	2021-12-15
Cert Version	Version: 1 Will be superseded by Baltimore CyberTrust root which is version 3.	3	3
Modulus length	1024 NIST recommended that all 1024 bit roots be phased out by the end of 2010, yet this root expires in 2018. There are still many mobile devices in APAC that cannot handle 2048-bit keys. Current web server technology forces our customers to make a choice between EV and mobile support. In the APAC market, the majority of SSL terminations are with a mobile device. Without enabling EV on a 1024 bit root, we obstruct APAC market adoption of EV. The JCAF has made similar comments in this regard in the CAB Forum discussion lists.	2048	2048
CRL URL	http://www.public-trust.com/cgi-bin/CRL/2018/cdp.crl http://crl.globalsign.net/sureserver.crl	http://www.public-trust.com/cgi-bin/CRL/202501/cdp.crl	http://www2.public-trust.com/ctroot.crl http://crl.omniroot.com/ctglobal.crl http://crl.omniroot.com/SureServerEV.crl
CRL update frequency for end-entity certs	CRL issuing frequency for end-entity certificates: every three hours with four day grace period for DR/BCP		
OCSP Responder URL	Not applicable	not applicable	not applicable

Subordinate CAs operated internally	The internally operated sub-CAs under the GTE CyberTrust Global Root are: - Cybertrust SureServer Standard Validation CA - Cybertrust Surecredential CA - Cybertrust SureCodesign CA - **Cybertrust SureServer EV CA -- relies on the Cybertrust Global Root's cross-certificate to the GTE CyberTrust Global Root for legacy browsers** The CP, CPS and audits cover all of these.	Currently no subordinate CAs have been issued under the Baltimore CyberTrust Root. We do not yet have any operational subordinate CAs under this root. Over time, we will migrate the internal and external hierarchies under the GTE CyberTrust Global Root to this root. This root will issue the same brands and types of certificates as the GTE CyberTrust Global Root currently does once it supersedes the GTE root. When that happens, the internally operated sub-CAs will be: - Cybertrust SureServer Standard Validation CA - Cybertrust Surecredential CA - Cybertrust SureCodesign CA - Cybertrust SureServer EV CA -- relies on the Cybertrust Global Root's cross-certificate to the GTE CyberTrust Global Root for legacy browsers The CP, CPS and audits cover all of these.	This Cybertrust Global Root has one internally-operated subordinate CA, the Cybertrust SureServer EV CA. This sub-CA will only issue EV SSL server certificates. This root is cross-certified by the GTE CyberTrust Global Root. It has issued one subordinate CA for internal use, the Cybertrust SureServer EV CA. In response to a completed WebTrust EV point in time readiness check, it has issued one subordinate CA for reseller use.
Subordinate CAs operated by third parties	The GTE CyberTrust Global Root has signed sub-CAs that are operated by third parties. However, no list has been provided due to confidentiality.	There are currently no subordinate CAs under the Baltimore CyberTrust Root at this time. This root will issue the same sub-CA's that are operated by 3rd-parties as the GTE CyberTrust Global Root currently does once it supersedes the GTE root. The Belgian government intends to move their eID program under this root.	In response to a completed WebTrust EV point in time readiness check, it has issued one subordinate CA for reseller use.
Subordinate CAs operated	The following is from the GTE CyberTrust Global Root, and will also apply to the Baltimore CyberTrust Root:		

by third parties **for internal use**	The subordinates issued to customer premise CAs are for enterprise usage only and subject to annual internal audits, net worth requirements, and multimillion dollar general liability and errors and omissions insurance coverage. CyberTrust retains the right to make an enterprise customer conduct an external audit at their cost if they have reason to suspect compliance issues. The number of sub-CAs operated at enterprise customers for their own use would be approximately 35. We prefer path length zero to restrict further subordinates, but we accept a practice whereby the customer attests that they will only operate the intermediate tier in an offline manner. We also always limit use to within arms length of the enterprise.	
Subordinate CAs operated by third parties **for reseller purposes**	The following is from the GTE CyberTrust Global Root, and will also apply to the Baltimore CyberTrust Root: There are also subordinates issued to commercial reseller CAs who are required to pass WebTrust audits annually. The number of resellers is 5. Specific customer identification is intellectual property which can be disclosed under NDA. Resellers are allowed to issue subordinate CAs to create separate classes of certificate issuers, but are contractually blocked from establishing subordinates operated by any other organization, even if at reseller premises. Several of these organizations are undergoing their first audits and/or point in time audits. The subordinate CAs inherit the CyberTrust CP and CPS and they are required to pass WebTrust against it in all but the oldest legacy cases where CyberTrust conducts their own audits onsite directly. At most once per week the CyberTrust security team exposes the root for customer subordination. CyberTrust strongly recommends that the customers operate one tier offline and manage online issuing CAs under that. CyberTrust supports them with path length constraint of 1 just for that purpose.	
Audits of Subordinate CAs operated by third parties	Resellers are required to pass WebTrust. We are in the process of moving our legacy resellers to WebTrust audit, these audits are currently in progress.	Resellers are required to pass WebTrust.

EV-enabled Subordinate CAs operated by third parties	Are any of the sub-CAs that are operated by third-parties are or will be EV enabled? If the answer is yes, then please refer to http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf section 7.b.1 and section 37b. From Steven Medin: “That is language that is very deeply understood and contemplated before we enabled our partner to issue EV SSL. Had we not had such a long working relationship, we would not have taken the risk to assume responsibility for their warranties and the critical findings in their WT/EVCA audits. I commit that we entirely understand our obligations and fully support the language in the Guidelines. Our partner is obligated to perform exactly as we are, they are bound to the same CPS and audited against it. By this equal treatment, we suggest that we can use one OID to denote the policy even though two parties perform under it. It is clear through the differing subordinate CAs which party is responsible for issuance. We further understand that this presents a risk if our partner fails to satisfy Foundation requirements and needs to be pulled from Firefox because using a single OID does not offer granularity to remove them but keep us. We suggest that in such a case we would revoke the partner's CA certificate.” From Kathleen: I have reviewed the information provided by Steven Medin, including one of the service description documents, and have confirmed the information below. From Steven Medin: “The attached service description document is bound by reference into the terms and conditions that form the master service agreement with any reseller that operates a subordinate CA at their premises that is chained to the GTE CyberTrust Global Root and its successors. At section 2.3.5 find the stated requirement of WebTrust audit. Our term Service Description does not imply marketing collateral, rather it details the legal specifics of a certain service while relying on the MSA for the typical legal language about the general business relationship. It is a binding part of the MSA. That service description is used for resellers that wish to issue SSL certificates which are NOT marked with EV SSL issuance ability. It requires an initial and annual WT/CA audit. It does not require an annual WT/EVCA audit because it does not grant EV issuance ability. Before we will allow a reseller to issue EV SSL certificates, they must first have a completed WT/CA audit and a WT/EVCA point in time readiness check. They must annually pass their WT/CA and WT/EVCA audits. Their WT/EVCA audits become incorporated by reference into our WT/EVCA audit – we are directly responsible for resolution of their critical findings. Because we expect very limited business relationships so strong that we will convey EV issuing privilege, we do not have prepackaged standard language defining the responsibilities of the parties in this case. We currently have one reseller who has an EV-enabled subordinate CA.”

List any other root CAs that have issued cross-signing certificates for this root CA	The Extended Validation CA is signed under Cybertrust Global Root, and that root is cross-certified to this GTE CyberTrust Global Root for the purposes of legacy ubiquity. Certain browser users who examine the certificate chain will see a four tier chain terminating in the GTE CyberTrust Global Root for certificates which have been issued according to the EV Guidelines.	The following will be inherited when this root supersedes the GTE CyberTrust Global Root: The Extended Validation CA is signed under Cybertrust Global Root, and that root is cross-certified to this GTE CyberTrust Global Root for the purposes of legacy ubiquity. Certain browser users who examine the certificate chain will see a four tier chain terminating in the GTE CyberTrust Global Root for certificates which have been issued according to the EV Guidelines. Yes, we will cross-certify the Cybertrust Global Root under the Baltimore CyberTrust Root.	This root is cross-certified by the GTE CyberTrust Global Root.
Requested Trust Bits: • Websites (SSL/TLS) • Email (S/MIME) • Code Signing	Websites Email Code Signing Currently the Websites and Email trust bits are enabled in the GTE CyberTrust Global Root built-in object. This request is to also enable the Code Signing trust bit.	Websites Email Code Signing Currently only the Websites trust bit is enabled in the Baltimore CyberTrust Root built-in object. This request is to also enable the Email and Code Signing trust bits.	Websites
SSL Validation DV, OV, EV	OV, EV	OV, EV	EV
CPS SureServer	1.5 SureServer SureServer certificates validity period is between one and three years according to the choice of the applicant. SureServer certificates are issued to legal entities and self employed professionals registered with a professional organisation. 1.5.7 Issuing Procedure The following steps describe the milestones in the procedure to issue aa SureServer certificate is as follows: 1 The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.		

	2 The applicant follows the on line registration procedure. 3 The applicant submits the required information including organizational information, technical contact, server information, payment information. 4 The applicant accepts the on line subscriber agreement. 5 Data is sent with certificate request to Cybertrust automatically. 6 Cybertrust verifies the submitted information by checking organisational, payment and any other information as it sees fit. This may also include checks in third party databases or resources. 7 Cybertrust may positively verify the applicant. 8 Cybertrust may issue the certificate to the applicant. 9 Cybertrust publishes the issued certificate in online database 10 Renewal: allowed 11 Revocation: allowed Cybertrust might apply variations of this procedure in order to meet service, standards or legal requirements.
CPS SureServer EV	1.6 SureServer EV 1.6.5 Data Verification As to data verification, Cybertrust ensures that the following Subject organization information has been submitted by the applicant and shall be verified by the CA in accordance with the EV Guidelines (Sections 14 through 25) by taking all verification steps reasonably necessary: 1 Applicant’s existence and identity, including: (a) Applicant’s legal existence and identity (as established with an Incorporating Agency), (b) Applicant’s physical existence (business presence at a physical address), and (c) Applicant’s operational existence (business activity) 2 Applicant’s exclusive control of the domain name to be included in certificate; 3 Applicant’s authorization for the SureServer EV certificate, including; (a) Contract Signer, certificate Approver and certificate Requester name, title, and authority (b) Subscriber Agreement signing by Contract Signer (c) Approval by the certificate Approver of the certificate Request. In this regard, Cybertrust acknowledges that a satisfactory data verification process requires an appropriate assessment of the legal and administrative practices that are applicable in the applicant’s jurisdiction. Cybertrust shall consequently take all reasonable steps to conform to the said practices. In all cases, Cybertrust is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the EV Guidelines Verification Requirement (e.g. Verification through verified Legal Opinion, verified Accountant letter, or other Qualified Independent Information Sources or Qualified Government Information source). In addition, Cybertrust shall take reasonable steps to identify Applicants likely to be at a high risk of being targeted for fraudulent attacks (phishing and other fraudulent schemes), and conduct such additional verification activity and take such additional precautions as are reasonably necessary to ensure that such Applicants are properly verified under the EV Guidelines.

EV policy OID(s)	1.3.6.1.4.1.6334.1.100.1	1.3.6.1.4.1.6334.1.100.1	1.3.6.1.4.1.6334.1.100.1
Example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s) where applicable.	https://cybertrust.omniroot.com The site listed is certified by the Cybertrust SureServer CA, which is signed by this GTE CyberTrust Global Root.	Unable to complete This root presently has no subordinate CAs issued and only limited directly issued SSL server certificates used in internal testing environments at this time. The root is already embedded in Firefox. From Steven Medin on 10/17/08: “We are presently unable to do so. We do not have internal testing certs against this root. To do so would require a secure facility transaction and to the best of our ability we limit those to only required events to satisfy customer requirements**.** If a test certificate is required, Mozilla may produce a PKCS#10 and we will schedule creation of a 30 day lifespan test. That test will not accurately reflect our eventual production operation through a tier or tiers of intermediate CAs, but rather be directly issued from the root. We strongly recommend that Mozilla may rely upon our interoperability expertise and the maturity of x.509 to be assured of proper operation with certificates issued from this root.”	https://shopping.discovery.com This site is certified by the Cybertrust SureServer EV CA, which is signed by the Cybertrust Global Root and the GTE CyberTrust Global Root.
CP/CPS	http://cybertrust.omniroot.com/repository Updated CPS: http://cybertrust.omniroot.com/repository/Cybertrust_CPS_v_5_4.pdf Update link to CP: http://cybertrust.omniroot.com/repository/Cybertrust_CP_v_2_3_cl.pdf		

	We operate a single consolidated CP and CPS for all our public operations that treats all our roots like interchangeable commodities. We do not operate different tiers of trust under different embedded roots, rather we operate different product brands and it is in those brands that we distinguish our assurances. For example, we don't have a "class 3 root," we implement class at the intermediate CA level. We will provide the same assurance SureCredential user certificate under the Baltimore root as we do under the GTE root.
AUDIT	Audit Type (WebTrust, ETSI etc.): WebTrust CA Auditor: Ernst and Young Auditor Website: www.ey.com/be WT/CA audit, 2008: https://cert.webtrust.org/SealFile?seal=799&file=pdf. 7/28/2008 Our assertion is limited to the following Root and Issuing CA's: The "Cybertrust Global Root" The "GTE CyberTrust Global Root" We have not yet moved to the Baltimore CyberTrust Root, it remains long-term vaulted, and has no operational CAs at this time. WT/EV audit, 2008: https://cybertrust.omniroot.com/repository/WT_EV_2008_SealFile.pdf 7/28/2008 For: Cybertrust Global Root CA Only the Cybertrust Global Root issues operational EV CAs. A quick comment on our path of ownership: our audit names Cybertrust Belgium NV and that is the entity that runs the Leuven, Belgium secure facility where we operate our CA practice. It is owned by the US corporation Verizon Business Network Services LLC, which is owned by a variety of parent tiers pointing ultimately to the public company that holds Verizon Business, Verizon Wireless and the US telecom. From: Christel Weymeersch <christel.weymeersch@be.ey.com> Subject: Fw: Verifying Authenticity of Cybertrust audit for Webtrust EV To: "Kathleen Wilson" <kathleen95014@yahoo.com> Date: Tuesday, November 18, 2008, 10:37 PM Dear Kathleen I can hereby confirm to you that I have signed the EY report on the Cybertrust audit mentioned below and can confirm the seal.

Review CPS sections dealing with subscriber verification (COMPLETE)
(section 7 of http://www.mozilla.org/projects/security/certs/policy/)

- Verify domain check for SSL
    - CPS section 1.5.7, SureServer Issuing Procedures:
        - Cybertrust verifies the submitted information by checking organisational, payment and any other information as it sees fit. This may also include checks in third party databases or resources.
    - CPS section 1.6.5, SureServer EV Data Verification
        - As to data verification, Cybertrust ensures that the following Subject organization information has been submitted by the applicant and shall be verified by the CA in accordance with the EV Guidelines (Sections 14 through 25) by taking all verification steps reasonably necessary:
        - 1 Applicant's existence and identity, including: (a) Applicant's legal existence and identity (as established with an Incorporating Agency), (b) Applicant's physical existence (business presence at a physical address), and (c) Applicant's operational existence (business activity)
        - 2 Applicant's exclusive control of the domain name to be included in certificate;
    - CPS section 1.7.6 SureCredential Professional Issuing Procedure
        - Cybertrust verifies the submitted information by checking organisational and any other information as it sees fit. This may also include checks in third party databases or resources and independent verification through telephone.
- Verify the email account associated with the email address in the cert is owned by the subscriber. In addition to verification of subscriber's legal identity.
    - CPS section 1.3.7, Issuing Procedure
        - The following steps describe the milestones in the procedure to issue a SureCredential Personal certificate:
        - 1 The applicant chooses a strong password and submits it to an online web form along with the email address they wish to have certified by Cybertrust.
        - 2 The automated system informs the applicant to check the inbox for the specified email address for further instructions.
        - 3 When the applicant receives an email from the automated system, it contains a unique single use URL which the applicant is instructed to click on or load in their browser to continue.
    - CPS section 1.4.6, Issuing Procedure
        - The following steps describe the milestones in the procedure to issue a SureCredential Professional certificate:
        - 1 The applicant chooses a strong password and submits it to an online web form along with the email address they wish to have certified by Cybertrust.
        - 2 The automated system informs the applicant to check the inbox for the specified email address for further instructions.
        - 3 When the applicant receives an email from the automated system, it contains a unique single use URL which the applicant is instructed to click on or load in their browser to continue.
- Verify identity info in code signing certs is that of subscriber
    - CPS section 1.8, SureCodesign Issuing Procedure
        - The procedure for a certificate request can be summarized as follows:

        - 1 The applicant fills out online the registration form: e-mail address, organizational info, common name, country code, payment info
        - 2 The applicant accepts the online subscriber agreement
        - 3 A key pair is generated on an applicant’s device (e.g. computer, smart card device etc.)
        - 4 The public key and online request are sent to Cybertrust automatically
        - 5 Cybertrust verifies the submitted information by checking organisational, payment and any other information as it sees fit also through third party databases or resources. This may also include checks in third party databases or resources and independent verification through telephone.
        - 6 Cybertrust may positively verify the applicant.

Flag Problematic Practices (COMPLETE)
(http://wiki.mozilla.org/CA:Problematic_Practices)

- Long-Lived Domain-Validated SSL certs
    - All SSL certs under these roots are OV or EV.
- Wildcard DV SSL certs
    - All SSL certs under these roots are OV or EV.
- Issuing end entity certs directly from root rather than using an offline root and issuing certs through a subordinate CA
    - Their cert hierarchy is such that certs are usually issued through the subordinate CAs.
        - “We only issue testing certificates in volumes less than 5 per year directly from the Baltimore CyberTrust Root in response to specific testing requirements from user agent vendors who wish to test against that specific root because it does not have any public issuance.
- Allowing external entities to operate subordinate CAs
    - Sub-CAs are operated by external parties (see above in regards to both resellers and enterprises with sub-CAs)
        - “We impose contractual limits that restrict resellers and enterprises to operate subordinate CAs entirely within their own organizational boundaries. In many cases, our customers wish to operate an offline tier at their location with operational subordinates under it. This allows them to renew the operational tier more frequently without the additional effort of a signing transaction with us. We support that technically with path length 1. Our initial proposal to our customers is path length zero and variance is subject to our approval.
- Distributing generated private keys in PKCS#12 files
    - “We do not generate, hold, or distribute customer private keys in any form in the public trust services under our widely embedded roots.”
- Certificates referencing hostnames or private IP addresses
    - “We require strictly FQDNs as the common names and subject alternate names in our public trust services. We do not issue IP CNs or SANs.”
- OCSP Responses signed by a certificate under a different root
    - Not applicable
- CRL with critical CIDP Extension
    - CRL successfully downloaded into Firefox

Verify Audits (COMPLETE)

- Validate contact info in report, call to verify that they did indeed issue this report.
  - Complete
- For EV CA’s, verify current WebTrust EV Audit done.
  - Complete
- Review Audit to flag any issues noted in the report
  - Complete, no issues noted in report.