Mozilla - CA Program

Case Information

Case Number	00000068	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Trend Micro	**Request Status**	Need Information from CA

Additional Case Information

Subject	Enable Email and Code Signing Trust bits for included roots	**Case Reason**	

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org/show_bug.cgi?id=1196376

General information about CA's associated organization

CA Email Alias 1	ssl_root_admin@trendmicro.com		
CA Email Alias 2			
Company Website	http://webappsecurity.trendmicro.com/	**Verified?**	Verified
Organizational Type	Commercial Organization	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	United States	**Verified?**	Verified
Primary Market / Customer Base	NEED: item 4 of https://wiki.mozilla.org/CA:Information_checklist#General_information_about_the_associated_organization_of_the_CA	**Verified?**	Need Response From CA
Impact to Mozilla Users	The AffirmTrust root certs were included via Bugzilla Bug #543639, with the Websites trust bit enabled. This request is to enable the Email and Code Signing trust bits for those root certs.	**Verified?**	Verified

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	NEED: Review and respond to https://wiki.mozilla.org/CA:Recommended_Practices#CA_Recommended_Practices * Publicly Available CP/CPS: Yes * CA Hierarchy: yes * Audit Criteria: yes * Document handling of IDNs in CP/CPS: ? (not applicable?)	**Verified?**	Need Response From CA

* Revocation of Compromised Certificates: CPS section 4.9.1
* Verifying Domain Name Ownership: Yes
* Verifying Email Address Control: Yes
* Verifying Identity of Code Signing Cert Subscriber: Yes
* DNS names go in SAN: CPS section 3.1.1
* Domain owned by a Natural Person: ?
* OCSP: ?
* 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	NEED: Review and respond to https://wiki.mozilla.org/CA:Problematic_Practices#Potentially_problematic_CA_practices * Long-lived DV Certs: Up to 39 months for OV; 27 months for EV * Wildcard Certs: ? * Email address prefixes for DV Certs: CPS section 3.2.2.1 * Delegation of Domain/Email Validation to third parties: ? * Issuing end-entity certs directly from root: no * Allowing external entities to operate subCA: ? * Distributing generated private keys in a PKCS#12 file: ? * Certificates referencing hostnames or private IP addresses: ? * Issuing SSL certs for internal domains: ? * OCSP responses signed by a cert under a different root: No * SHA-1 Certs: http://www.trendmicro.com/cloud-content/us/pdfs/business/faqs/tm_deprecation_of_sha-1.pdf * Generic names for CAs: No * Lack of Communication with end users: ? * Backdating the notBefore date: ?	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Certificate Name	AffirmTrust Commercial	**Root Case No**	R00000092
Request Status	Need Information from CA	**Case Number**	00000068

Additional Root Case Information

Subject	Enable trust bits for AffirmTrust Commercial root

Technical Information about Root Certificate

O From Issuer Field	AffirmTrust	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root cert was included via Bugzilla Bug #543639, with the Websites trust bit enabled. This request is to enable the Email and Code Signing trust bits.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=425501	**Verified?**	Verified
Valid From	2010 Jan 29	**Verified?**	Verified

Valid To	2030 Dec 31	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-256	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://commercial.affirmtrust.com/	**Verified?**	Verified
CRL URL(s)	http://crl.affirmtrust.com/crl/AffirmTrustCommercial.crl http://crl.affirmtrust.com/crl/aftcomev2.crl (NextUpdate: 7 days)	**Verified?**	Verified
OCSP URL(s)	http://ocsp.affirmtrust.com/commev	**Verified?**	Verified
Revocation Tested	NEED: Resolve errors https://certificate.revocationcheck.com/commercial.affirmtrust.com NEED: Why doesn't AffirmTrust Commercial Extended Validation CA have the OCSP URI in the AIA?	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.34697.2.1	**Verified?**	Verified
EV Tested	NEED successful test output from https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version Note: Whenever a CA applies to change a root (e.g. add trust bits, etc) Mozilla's process requires re-evaluation of the root and all the trust bits and EV treatment (when applicable). When I tried the EV test, I got this error: BuildCertChain failed: SEC_ERROR_UNKNOWN_ISSUER which usually means the webserver is not serving up the intermediate cert.	**Verified?**	Need Response From CA
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	F9:B5:B6:32:45:5F:9C:BE:EC:57:5F:80:DC:E9:6E:2C:C7:B2:78:B7	**Verified?**	Verified
SHA-256 Fingerprint	03:76:AB:1D:54:C5:F9:80:3C:E4:B2:E2:01:A0:EE:7E:EF:7B:57:B6:36:E8:A9:3C:9B:8D:48:60:C9:6F:5F:A7	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED confirm or update: AffirmTrust Commercial sub-CAs: - AffirmTrust Commercial Extended Validation – for signing EV SSL end-entity certs. - AffirmTrust Commercial OV Sub-CA – for signing Organization Validated end-entity certs.	**Verified?**	Need Response From CA

	- AffirmTrust Commercial DV Sub-CA – for signing Domain Validated end-entity certs. - End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Commercial [additional information re sub-CA and authentication method]. Key length will be 2048 bits.		
Externally Operated SubCAs	NEED info about externally-operated subCAs as per #2 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA
Cross Signing	CPS Appendix A.4: "Trend Micro S2 CA" is signed by both "AffirmTrust Commercial" and "SwissSign Gold CA-G2"	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	NEED info about technical constraints on 3rd-party issuers as per #4 of NEED: CA Hierarchy info as per #1 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate CPS section 1.3.1: Trend Micro SSL Server Certificates are X.509 Certificates with SSL Extensions issued from sub-roots that chain and may be cross-signed to the trusted roots listed on Appendix A CPS section 1.3.2: Trend Micro does not use external Registration Authorities.	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	All documents are in English.	**Verified?**	Verified
CA Document Repository	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CP	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-cps-v2_1-effective-12-august-2015.pdf	**Verified?**	Verified
Other Relevant Documents	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-relying-party-agreement-v1.3-effective-17-february-2014.pdf	**Verified?**	Verified
Auditor Name	Grant Thornton	**Verified?**	Verified
Auditor Website	http://www.grantthornton.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1894&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1896&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/30/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1895&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.3.1	**Verified?**	Verified

SSL Verification Procedures	CPS section 3.2.2.1: Trend Micro also validates the Applicant’s right to use the domain name that will be listed in the certificate. Domain name ownership is validated by: (a) Relying on publicly available records from the Domain Name Registrar. Trend Micro compares WhoIs Registrant information with the confirmed Organization identity information obtained for the Applicant under Section 3.2.2 using matching algorithms that include name, address, and other information. In the event of doubt, Trend Micro additionally requires use of the domain control confirmation methods stated in subsections (b) or (c). Trend Micro periodically correlates multiple sources to confirm the integrity of the WhoIs information used; or (b) Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain.com, postmaster@domain.com, and any address listed in the technical, registrant, or administrative contact field of the domain’s Domain Name Registrar record; or (c) Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain).	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.2.2.2	**Verified?**	Verified
Organization Verification Procedures	CPS section 3.2.2 - Authentication of Organization Identity CPS section 3.2.3: Trend Micro does not issue SSL server certificates to individuals.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2.4: Trend Micro will verify that the Applicant 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 by sending an email to the address to be included in the certificate containing secret unpredictable information and giving the Applicant a limited time to use the information by sending a return email or using a web-based application to respond to the email and including the secret unpredictable information provided by Trend Micro.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	CPS section 3.2.2.3 and 3.2.5.1	**Verified?**	Verified
Multi-Factor Authentication	NEED confirmation that multi-factor authentication is required for all accounts capable of directly causing certificate issuance as per #6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	CPS section 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to a web page or a Bugzilla Bug Number that lists all publicly disclosed sub-CA certs that chain up to this root, as per #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA

Root Case Record # 2

Root Case Information

Root Certificate Name	AffirmTrust Networking	**Root Case No**	R00000093
Request Status	Need Information from CA	**Case Number**	00000068

Additional Root Case Information

Subject	Enable trust bits for AffirmTrust Networking root

Technical Information about Root Certificate

O From Issuer Field	AffirmTrust	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root cert was included via Bugzilla Bug #543639, with the Websites trust bit enabled. This request is to enable the Email and Code Signing trust bits.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=425501	**Verified?**	Verified
Valid From	2010 Jan 29	**Verified?**	Verified
Valid To	2030 Dec 31	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-1	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://networking.affirmtrust.com:4431/	**Verified?**	Verified
CRL URL(s)	http://crl.affirmtrust.com/crl/AffirmTrustNetworking.crl http://crl.affirmtrust.com/crl/aftnetworkev2.crl (NextUpdate: 7 days)	**Verified?**	Verified
OCSP URL(s)	http://ocsp.affirmtrust.com/ntwkev	**Verified?**	Verified
Revocation Tested	NEED: Resolve errors https://certificate.revocationcheck.com/networking.affirmtrust.com NEED: Why doesn't AffirmTrust Networking Extended Validation CA have the OCSP URI in the AIA?	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.34697.2.2	**Verified?**	Verified
EV Tested	NEED successful test output from https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version When I tried the EV test, I got this error: BuildCertChain failed: SEC_ERROR_CERT_BAD_ACCESS_LOCATION The location for the certificate status server has invalid format. It appears to be the case that a certificate in the issuance chain has a malformed or missing OCSP AIA URI	**Verified?**	Need Response From CA
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	29:36:21:02:8B:20:ED:02:F5:66:C5:32:D1:D6:ED:90:9F:45:00:2F	**Verified?**	Verified

SHA-256 Fingerprint	0A:81:EC:5A:92:97:77:F1:45:90:4A:F3:8D:5D:50:9F:66:B5:E2:C5:8F:CD:B5:31:05:8B:0E:17:F3:F0:B4:1B	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED confirm or update: AffirmTrust Networking sub-CAs: - AffirmTrust Networking Extended Validation – for signing EV SSL end-entity certs. - AffirmTrust Networking OV Sub-CA – for signing Organization Validated end-entity certs. - AffirmTrust Networking DV Sub-CA – for signing Domain Validated end-entity certs. - End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Networking [additional information re sub-CA and authentication method]. Key length will be 2048 bits.	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED info about externally-operated subCAs as per #2 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA
Cross Signing	CPS Appendix A.4: "Trend Micro S2 CA" is signed by both "AffirmTrust Networking" and "SwissSign Gold CA-G2"	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	NEED info about technical constraints on 3rd-party issuers as per #4 of NEED: CA Hierarchy info as per #1 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate CPS section 1.3.1: Trend Micro SSL Server Certificates are X.509 Certificates with SSL Extensions issued from sub-roots that chain and may be cross-signed to the trusted roots listed on Appendix A CPS section 1.3.2: Trend Micro does not use external Registration Authorities.	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	All documents are in English.	**Verified?**	Verified
CA Document Repository	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CP	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-cps-v2_1-effective-12-august-2015.pdf	**Verified?**	Verified
Other Relevant Documents	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-relying-party-agreement-v1.3-effective-17-february-2014.pdf	**Verified?**	Verified
Auditor Name	Grant Thornton	**Verified?**	Verified
Auditor Website	http://www.grantthornton.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1894&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1896&file=pdf	**Verified?**	Verified

BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/30/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1895&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.3.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.1: Trend Micro also validates the Applicant’s right to use the domain name that will be listed in the certificate. Domain name ownership is validated by: (a) Relying on publicly available records from the Domain Name Registrar. Trend Micro compares WhoIs Registrant information with the confirmed Organization identity information obtained for the Applicant under Section 3.2.2 using matching algorithms that include name, address, and other information. In the event of doubt, Trend Micro additionally requires use of the domain control confirmation methods stated in subsections (b) or (c). Trend Micro periodically correlates multiple sources to confirm the integrity of the WhoIs information used; or (b) Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain.com, postmaster@domain.com, and any address listed in the technical, registrant, or administrative contact field of the domain’s Domain Name Registrar record; or (c) Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain).	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.2.2.2	**Verified?**	Verified
Organization Verification Procedures	CPS section 3.2.2 - Authentication of Organization Identity CPS section 3.2.3: Trend Micro does not issue SSL server certificates to individuals.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2.4: Trend Micro will verify that the Applicant 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 by sending an email to the address to be included in the certificate containing secret unpredictable information and giving the Applicant a limited time to use the information by sending a return email or using a web-based application to respond to the email and including the secret unpredictable information provided by Trend Micro.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	CPS section 3.2.2.3 and 3.2.5.1	**Verified?**	Verified
Multi-Factor Authentication	NEED confirmation that multi-factor authentication is required for all accounts capable of directly causing certificate issuance as per #6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	CPS section 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to a web page or a Bugzilla Bug Number that lists all publicly disclosed sub-CA certs that chain up to this root, as per #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA

Root Case Record # 3

Root Case Information

Root Certificate Name	AffirmTrust Premium	**Root Case No**	R00000094
Request Status	Need Information from CA	**Case Number**	00000068

Additional Root Case Information

Subject	Enable trust bits for AffirmTrust Premium root

Technical Information about Root Certificate

O From Issuer Field	AffirmTrust	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root cert was included via Bugzilla Bug #543639, with the Websites trust bit enabled. This request is to enable the Email and Code Signing trust bits.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=425501	**Verified?**	Verified
Valid From	2010 Jan 29	**Verified?**	Verified
Valid To	2040 Dec 31	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	SHA-384	**Verified?**	Verified
Signing Key Parameters	4096	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://premium.affirmtrust.com:4432/	**Verified?**	Verified
CRL URL(s)	http://crl.affirmtrust.com/crl/AffirmTrustPremium.crl http://crl.affirmtrust.com/crl/aftpremev2.crl (NextUpdate: 7 days)	**Verified?**	Verified
OCSP URL(s)	http://ocsp.affirmtrust.com/premev	**Verified?**	Verified
Revocation Tested	NEED: Resolve errors https://certificate.revocationcheck.com/premium.affirmtrust.com NEED: Why doesn't AffirmTrust Premium Extended Validation CA have the OCSP URI in the AIA?	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.34697.2.3	**Verified?**	Verified
EV Tested	NEED successful test output from https://wiki.mozilla.org/PSM:EV_Testing_Easy_Version When I tried the EV test, I got this error: BuildCertChain failed: SEC_ERROR_CERT_BAD_ACCESS_LOCATION	**Verified?**	Need Response From CA

	The location for the certificate status server has invalid format. It appears to be the case that a certificate in the issuance chain has a malformed or missing OCSP AIA URI		
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	D8:A6:33:2C:E0:03:6F:B1:85:F6:63:4F:7D:6A:06:65:26:32:28:27	**Verified?**	Verified
SHA-256 Fingerprint	70:A7:3F:7F:37:6B:60:07:42:48:90:45:34:B1:14:82:D5:BF:0E:69:8E:CC:49:8D:F5:25:77:EB:F2:E9:3B:9A	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED confirm or update: AffirmTrust Premium planned sub-CAs: - AffirmTrust Premium Extended Validation – for signing EV SSL end-entity certs. - AffirmTrust Premium OV Sub-CA – for signing Organization Validated end-entity certs. - AffirmTrust Premium DV Sub-CA – for signing Domain Validated end-entity certs. - End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Premium [additional identity information re sub-CA and authentication method.] Key length will be 4096 bits.	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED info about externally-operated subCAs as per #2 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA
Cross Signing	CPS Appendix A.4: "Trend Micro S2 CA" is signed by both "AffirmTrust Premium," and "SwissSign Gold CA-G2"	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	NEED info about technical constraints on 3rd-party issuers as per #4 of NEED: CA Hierarchy info as per #1 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate CPS section 1.3.1: Trend Micro SSL Server Certificates are X.509 Certificates with SSL Extensions issued from sub-roots that chain and may be cross-signed to the trusted roots listed on Appendix A CPS section 1.3.2: Trend Micro does not use external Registration Authorities.	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	All documents are in English.	**Verified?**	Verified
CA Document Repository	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CP	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-cps-v2_1-effective-12-august-2015.pdf	**Verified?**	Verified

Other Relevant Documents	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-relying-party-agreement-v1.3-effective-17-february-2014.pdf	**Verified?**	Verified
Auditor Name	Grant Thornton	**Verified?**	Verified
Auditor Website	http://www.grantthornton.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1894&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1896&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/30/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1895&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.3.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.1: Trend Micro also validates the Applicant’s right to use the domain name that will be listed in the certificate. Domain name ownership is validated by: (a) Relying on publicly available records from the Domain Name Registrar. Trend Micro compares WhoIs Registrant information with the confirmed Organization identity information obtained for the Applicant under Section 3.2.2 using matching algorithms that include name, address, and other information. In the event of doubt, Trend Micro additionally requires use of the domain control confirmation methods stated in subsections (b) or (c). Trend Micro periodically correlates multiple sources to confirm the integrity of the WhoIs information used; or (b) Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain.com, postmaster@domain.com, and any address listed in the technical, registrant, or administrative contact field of the domain’s Domain Name Registrar record; or (c) Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain).	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.2.2.2	**Verified?**	Verified
Organization Verification Procedures	CPS section 3.2.2 - Authentication of Organization Identity CPS section 3.2.3: Trend Micro does not issue SSL server certificates to individuals.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2.4: Trend Micro will verify that the Applicant 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 by sending an email to the address to be included in the certificate containing secret unpredictable information and giving the Applicant a limited time to use the information by sending a return email or using a web-based application to respond to the email and including the secret unpredictable information provided by Trend Micro.	**Verified?**	Verified

Code Signing Subscriber Verification Pro	CPS section 3.2.2.3 and 3.2.5.1	**Verified?**	Verified
Multi-Factor Authentication	NEED confirmation that multi-factor authentication is required for all accounts capable of directly causing certificate issuance as per #6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	CPS section 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to a web page or a Bugzilla Bug Number that lists all publicly disclosed sub-CA certs that chain up to this root, as per #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA

Root Case Record # 4

Root Case Information

Root Certificate Name	AffirmTrust Premium ECC	**Root Case No**	R00000095
Request Status	Need Information from CA	**Case Number**	00000068

Additional Root Case Information

Subject	Enable trust bits for AffirmTrust Premium ECC root

Technical Information about Root Certificate

O From Issuer Field	AffirmTrust	**Verified?**	Verified
OU From Issuer Field		**Verified?**	Verified
Certificate Summary	This root cert was included via Bugzilla Bug #543639, with the Websites trust bit enabled. This request is to enable the Email and Code Signing trust bits.	**Verified?**	Verified
Root Certificate Download URL	https://bugzilla.mozilla.org/attachment.cgi?id=425501	**Verified?**	Verified
Valid From	2010 Jan 29	**Verified?**	Verified
Valid To	2040 Dec 31	**Verified?**	Verified
Certificate Version	3	**Verified?**	Verified
Certificate Signature Algorithm	ECC	**Verified?**	Verified
Signing Key Parameters	ECC P-384	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://premiumecc.affirmtrust.com:4433/	**Verified?**	Verified
CRL URL(s)	http://crl.affirmtrust.com/crl/AffirmTrustPremiumECC.crl http://crl.affirmtrust.com/crl/aftpremeccv2.crl (NextUpdate: 7 days)	**Verified?**	Verified

OCSP URL(s)	http://ocsp.affirmtrust.com/premeccev	**Verified?**	Verified
Revocation Tested	NEED: Resolve errors https://certificate.revocationcheck.com/premiumecc.affirmtrust.com NEED: Why doesn't AffirmTrust Premium ECC Extended Validation CA have the OCSP URI in the AIA?	**Verified?**	Need Response From CA
Trust Bits	Code; Email; Websites	**Verified?**	Verified
SSL Validation Type	DV; OV; EV	**Verified?**	Verified
EV Policy OID(s)	1.3.6.1.4.1.34697.2.4	**Verified?**	Verified
EV Tested	I'm checking on this -- may be that the EV Test Tool doesn't yet support ECC.	**Verified?**	Error
Root Stores Included In	Microsoft; Mozilla	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	B8:23:6B:00:2F:1D:16:86:53:01:55:6C:11:A4:37:CA:EB:FF:C3:BB	**Verified?**	Verified
SHA-256 Fingerprint	BD:71:FD:F6:DA:97:E4:CF:62:D1:64:7A:DD:25:81:B0:7D:79:AD:F8:39:7E:B4:EC:BA:9C:5E:84:88:82:14:23	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	NEED confirm or update: AffirmTrust Premium ECC planned sub-CAs: - AffirmTrust Premium ECC Extended Validation – for signing EV SSL end-entity certs. - AffirmTrust Premium ECC OV Sub-CA – for signing Organization Validated end-entity certs. - AffirmTrust Premium ECC DV Sub-CA – for signing Domain Validated end-entity certs. - End-entity certificates issued by any future external sub-CA will be issued off a sub-CA root certificate identified by sub-CA identity and authentication method with the following naming scheme: AffirmTrust Premium ECC [additional identity information re sub-CA and authentication method.] Key length will be 384 bits.	**Verified?**	Need Response From CA
Externally Operated SubCAs	NEED info about externally-operated subCAs as per #2 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA
Cross Signing	CPS Appendix A.4: "Trend Micro S2 CA" is signed by both "AffirmTrust Premium ECC" and "SwissSign Gold CA-G2"	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	NEED info about technical constraints on 3rd-party issuers as per #4 of NEED: CA Hierarchy info as per #1 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate CPS section 1.3.1: Trend Micro SSL Server Certificates are X.509 Certificates with SSL Extensions issued from sub-roots that chain and may be cross-signed to the trusted roots listed on Appendix A CPS section 1.3.2: Trend Micro does not use external Registration Authorities.	**Verified?**	Need Response From CA

Verification Policies and Practices

Policy Documentation	All documents are in English.	**Verified?**	Verified
CA Document Repository	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CP	http://webappsecurity.trendmicro.com/resources/	**Verified?**	Verified
CP Doc Language	English		
CPS	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-cps-v2_1-effective-12-august-2015.pdf	**Verified?**	Verified
Other Relevant Documents	http://www.trendmicro.com/cloud-content/us/pdfs/business/reports/trend-micro-relying-party-agreement-v1.3-effective-17-february-2014.pdf	**Verified?**	Verified
Auditor Name	Grant Thornton	**Verified?**	Verified
Auditor Website	http://www.grantthornton.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://cert.webtrust.org/SealFile?seal=1894&file=pdf	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Audit	https://cert.webtrust.org/SealFile?seal=1896&file=pdf	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	6/30/2015	**Verified?**	Verified
EV Audit	https://cert.webtrust.org/SealFile?seal=1895&file=pdf	**Verified?**	Verified
EV Audit Type	WebTrust	**Verified?**	Verified
EV Audit Statement Date	6/30/2015	**Verified?**	Verified
BR Commitment to Comply	CPS section 1.3.1	**Verified?**	Verified
SSL Verification Procedures	CPS section 3.2.2.1: Trend Micro also validates the Applicant’s right to use the domain name that will be listed in the certificate. Domain name ownership is validated by: (a) Relying on publicly available records from the Domain Name Registrar. Trend Micro compares WhoIs Registrant information with the confirmed Organization identity information obtained for the Applicant under Section 3.2.2 using matching algorithms that include name, address, and other information. In the event of doubt, Trend Micro additionally requires use of the domain control confirmation methods stated in subsections (b) or (c). Trend Micro periodically correlates multiple sources to confirm the integrity of the WhoIs information used; or (b) Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain.com, postmaster@domain.com, and any address listed in the technical, registrant, or administrative contact field of the domain’s Domain Name Registrar record; or (c) Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a live page on the given domain).	**Verified?**	Verified
EV SSL Verification Procedures	CPS section 3.2.2.2	**Verified?**	Verified

Organization Verification Procedures	CPS section 3.2.2 - Authentication of Organization Identity CPS section 3.2.3: Trend Micro does not issue SSL server certificates to individuals.	**Verified?**	Verified
Email Address Verification Procedures	CPS section 3.2.2.4: Trend Micro will verify that the Applicant 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 by sending an email to the address to be included in the certificate containing secret unpredictable information and giving the Applicant a limited time to use the information by sending a return email or using a web-based application to respond to the email and including the secret unpredictable information provided by Trend Micro.	**Verified?**	Verified
Code Signing Subscriber Verification Pro	CPS section 3.2.2.3 and 3.2.5.1	**Verified?**	Verified
Multi-Factor Authentication	NEED confirmation that multi-factor authentication is required for all accounts capable of directly causing certificate issuance as per #6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	CPS section 6	**Verified?**	Verified

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	NEED URL to a web page or a Bugzilla Bug Number that lists all publicly disclosed sub-CA certs that chain up to this root, as per #4 of https://wiki.mozilla.org/CA:Information_checklist#CA_Hierarchy_information_for_each_root_certificate	**Verified?**	Need Response From CA