Bugzilla ID: 606947
Bugzilla Summary: Add 3 COMODO Rollover Root CA Certificates and enable them for EV

CAs wishing to have their certificates included in Mozilla products must

1) Comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/)
2) Supply all of the information listed in http://wiki.mozilla.org/CA:Information_checklist.
    a. Review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices
    b. Review the Potentially Problematic Practices at https://wiki.mozilla.org/CA:Problematic_Practices

General information about the CA's associated organization

CA Company Name	COMODO
Website URL	http://www.comodo.com
Organizational type	Private Corporation
Primark Market / Customer Base	Comodo CA Ltd is a commercial CA based in the UK and serving customers worldwide.
Inclusion in other major browsers	Comodo root certs are included in the major browsers.
CA Primary Point of Contact (POC)	POC direct email: robin@comodo.com CA Email Alias: root.certificates@comodo.com CA Phone Number: 44 161 874 7070 Title / Department: CA Technical

Technical information about each root certificate

Certificate Name	COMODO RSA Certification Authority	USERTrust RSA Certification Authority	USERTrust ECC Certification Authority
Certificate Issuer Field	CN = COMODO RSA Certification Authority O = COMODO CA Limited L = Salford ST = Greater Manchester C = GB	CN = USERTrust RSA Certification Authority O = The USERTRUST Network L = Jersey City ST = New Jersey C = US	CN = USERTrust ECC Certification Authority O = The USERTRUST Network L = Jersey City ST = New Jersey C = US
Certificate Summary	This SHA-384 "COMODO RSA Certification Authority" root certificate will eventually replace the SHA-1 "COMODO Certification Authority" root certificate that was included via Bugzilla Bug #401587. Is the above statement correct?	This SHA-384 "USERTrust RSA Certification Authority" root certificate will eventually replace the SHA-1 "UTN-USERFirst-Hardware", "UTN - DATACorp SGC", "UTN-USERFirst-Client Authentication and Email", and "UTN-USERFirst-Object" root certificates that were included via Bugzilla Bug #242610. Is the above statement correct?	This "USERTrust ECC Certification Authority" root certificate is the ECC version of the "USERTrust RSA Certification Authority" root certificate. Is the above statement correct?
Root Cert URL	http://crt.comodoca.com/COMODORSACertificationAuthority.crt	http://crt.usertrust.com/USERTrustRSACertificationAuthority.crt	http://crt.usertrust.com/USERTrustECCCertificationAuthority.crt

SHA1 Fingerprint	AF:E5:D2:44:A8:D1:19:42:30:FF:47:9F:E2:F8:97:BB:CD:7A:8C:B4	2B:8F:1B:57:33:0D:BB:A2:D0:7A:6C:51:F7:0E:E9:0D:DA:B9:AD:8E	D1:CB:CA:5D:B2:D5:2A:7F:69:3B:67:4D:E5:F0:5A:1D:0C:95:7D:F0
Valid From	2010-01-19	2010-02-01	2010-02-01
Valid To	2038-01-18	2038-01-18	2038-01-18
Cert Version	3	3	3
Signature Algorithm	PKCS #1 SHA-384 With RSA Encryption	PKCS #1 SHA-384 With RSA Encryption	SECG elliptic curve secp384r1
Signing key parameters	4096	4096	NIST P-384
Test Website	https://comodorsacertificationauthority-ev.comodoca.com	https://usertrustrsacertificationauthority-ev.comodoca.com	https://usertrustecccertificationauthority-ev.comodoca.com
CRL URLs	http://crl.comodoca.com/COMODORSACertificationAuthority.crl http://crl.comodoca.com/COMODORSAExtendedValidationSecureServerCA.crl	http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl http://crl.usertrust.com/USERTrustRSAExtendedValidationSecureServerCA.crl	http://crl.trust-provider.com/USERTrustECCCertificationAuthority.crl http://crl.trust-provider.com/USERTrustECCExtendedValidationSecureServerCA.crl
OCSP URL	http://ocsp.comodoca.com OCSP responses for end entity certificates are regenerated every 24 hours. The OCSP responses show a 'Next Update' date 4 days after 'This Update' date.	http://ocsp.usertrust.com OCSP responses for end entity certificates are regenerated every 24 hours. The OCSP responses show a 'Next Update' date 4 days after 'This Update' date.	http://ocsp.trust-provider.com OCSP responses for end entity certificates are regenerated every 24 hours. The OCSP responses show a 'Next Update' date 4 days after 'This Update' date.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type	DV, OV, and EV	DV, OV, and EV	DV, OV, and EV
EV Policy OID(s)	1.3.6.1.4.1.6449.1.2.1.5.1 EV test completed: https://bugzilla.mozilla.org/attachment.cgi?id=8334937	1.3.6.1.4.1.6449.1.2.1.5.1 EV test completed: https://bugzilla.mozilla.org/attachment.cgi?id=8334939	1.3.6.1.4.1.6449.1.2.1.5.1 EV test completed: https://bugzilla.mozilla.org/attachment.cgi?id=8334941
CA Hierarchy	"COMODO RSA Certification Authority" currently has the following internally-operated sub-CAs: - COMODO RSA Extended Validation Secure Server CA - COMODO RSA Client Authentication and Secure Email CA	"USERTrust RSA Certification Authority" currently has the following internally-operated subCA: - USERTrust RSA Extended Validation Secure Server CA The following internally-operated sub-CAs	"USERTrust ECC Certification Authority" currently has the following internally-operated sub-CA: - USERTrust ECC Extended Validation Secure Server CA The following internally-operated sub-CAs

	- COMODO RSA Code Signing CA The following internally-operated sub-CAs are also planned: - (name tbd) for OV Server certificates - (name tbd) for DV Server certificates - (names tbd) to partition the sales of resellers, some bearing the name of the reseller in the subject and others bearing the Comodo name.	are also planned: - USERTrust RSA Client Authentication and Secure Email CA - USERTrust RSA Code Signing CA - (name tbd) for OV Server certificates - (name tbd) for DV Server certificates - (names tbd) to partition the sales of resellers, some bearing the name of the reseller in the subject and others bearing the UserTrust name.	are also planned: - USERTrust ECC Client Authentication and Secure Email CA - USERTrust ECC Code Signing CA - (name tbd) for OV Server certificates - (name tbd) for DV Server certificates - (names tbd) to partition the sales of resellers, some bearing the name of the reseller in the subject and others bearing the UserTrust name.
Externally Operated SubCAs	There are currently no externally operated sub-CAs issued from this root, but if we issue any they will be operated in accordance with Mozilla's CA Certificate Policy and will either be technically constrained or be publicly disclosed and audited. Are there currently externally-operated subCAs under the "COMODO Certification Authority" root certificate that will be transitioned to this root? Can you make a statement such as: Previously, externally-operated subCAs have been overseen via contractual controls or technical monitoring, supported by internal audit. Comodo is in the process of transitioning these clients before May 15, 2014 to either technical controls (nameConstraints) or audit with public disclosure as specified in Section 9 of the Mozilla CA Inclusion Policy.	There are currently no externally operated sub-CAs issued from this root, but if we issue any they will be operated in accordance with Mozilla's CA Certificate Policy and will either be technically constrained or be publicly disclosed and audited. Are there currently externally-operated subCAs under the existing "UTN ..." root certificates that will be transitioned to this root? Can you make a statement such as: Previously, externally-operated subCAs have been overseen via contractual controls or technical monitoring, supported by internal audit. Comodo is in the process of transitioning these clients before May 15, 2014 to either technical controls (nameConstraints) or audit with public disclosure as specified in Section 9 of the Mozilla CA Inclusion Policy.	There are currently no externally operated sub-CAs issued from this root, but if we issue any they will be operated in accordance with Mozilla's CA Certificate Policy and will either be technically constrained or be publicly disclosed and audited.
Cross-Signing	"COMODO RSA Certification Authority" is cross-signed with Comodo's "AddTrust External CA Root" (sha1 fingerprint: 02:fa:f3:e2:91:43:54:68:60:78:57:69:4d:f5:e4:5b:68:85:18:68, already in Mozilla's root program) "COMODO RSA Certification Authority" has not been cross-signed by any other CAs, and there are no plans to do so.	"USERTrust RSA Certification Authority" is cross-signed with Comodo's "AddTrust External CA Root" (sha1 fingerprint: 02:fa:f3:e2:91:43:54:68:60:78:57:69:4d:f5:e4:5b:68:85:18:68, already in Mozilla's root program) "USERTrust RSA Certification Authority" has not been cross-signed by any other CAs, and there are no plans to do so.	"USERTrust ECC Certification Authority" is cross-signed with Comodo's "AddTrust External CA Root" (sha1 fingerprint: 02:fa:f3:e2:91:43:54:68:60:78:57:69:4d:f5:e4:5b:68:85:18:68, already in Mozilla's root program) "USERTrust ECC Certification Authority" has not been cross-signed by any other CAs, and there are no plans to do so.

Verification Policies and Practices

Policy Documentation	All documents are in English. Repository: http://www.comodo.com/about/comodo-agreements.php CPS: http://www.comodo.com/repository/Comodo_CA_CPS_4.0.pdf EV SSL CPS: http://www.comodo.com/repository/EV_CPS_4_JUN_07.pdf Addendum to EV SSL CPS: http://www.comodo.com/repository/EV_CPS_Amendment-June_2009.pdf ECC addendum to EV SSL CPS: http://www.comodo.com/repository/ECC_addendum_to_the_EV_Certification_Practice_Statement.pdf Our current CPS is http://www.comodo.com/repository/Comodo_CA_CPS_4.0.pdf We are (as of Nov 11 2013) preparing a new version of the CPS which will include mention of these new roots.
Audits	Auditor: Ernst & Young WebTrust CA audit statement: http://cert.webtrust.org/SealFile?seal=1409&file=pdf (2012.11.20) WebTrust EV audit statement: http://cert.webtrust.org/SealFile?seal=1410&file=pdf (2012.11.20) From this year, 2013, we will have audit reports for WebTrust for CAs WebTrust SSL Baseline Requirements WebTrust Extended Validation and all three will show these three new roots as being in-scope for the issuance of certificates under the corresponding criteria (being publicly trusted certificates in general, publicly trusted certificates for server authentication, and Extended Validation certificates for server authentication). We expect to have the next audit reports for WebTrust for CAs and WebTrust for EV by thanksgiving this year, and the report for WebTrust for BRs by the end of 2013.
Baseline Requirements (SSL)	CPS section 1.1.1: Comodo conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event CA / Browser Forum Baseline Requirements, v. 1.0 8 of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.
Organization Verification Procedures	CPS section 4.2.1 EV SSL CPS section 4.2
SSL Verification Procedures	CPS section 4.2.1, Secure Server Certificates Validation Process: Comodo utilizes a two-step validation process prior to the issuance of a Secure Server Certificate, or three-step process prior to issuing a Code Signing Certificate. This process involves Comodo, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) for the following : 1. That the applicant has the right to use the domain name in the application (or, in the case of Code Signing Certificates, the domain name used in the application email address, i.e., for email address someone@example.com, applicant must demonstrate exclusive control of example.com), which is validated by:

	i. Reviewing domain name ownership records available publicly through Internet or approved global domain name registrars, or ii. For government and educational institution associated with a .EDU or .GOB domain only, receiving a letter on official departmental letterhead, with the order details and a statement verifying that the signor (which must be a WHOIS contact or senior member of management) is authorized to act on behalf of the organization. iii. Validation may also be supplemented: (1) by sending an email to a generic address only available to the person(s) controlling the domain name administration, e.g., webmaster@example.com, postmaster@example.com, admin@example.com, etc. or (2) direct communication with the administrator associated with the domain name register record. 2. To authenticate the identity of the certificate requestor, which is done by one of the following: i. For organization entities, identity is authenticated by using at least one third party database or service, or organizational documentation filed or issued with a government agency or competent authority, or ii. For non-organization individuals, identity is authenticated by documentation such as a bank statement, passport, driving license, or other such documents. 3. When validating Code Signing Certificates, the applicant will be contacted at a verified telephone number to confirm that the applicant requested the Certificate, and in the case of organizations, that the person submitting the application on behalf of that organization is authorized to do so. Telephone numbers are verified through third party databases or submission of a telephone bill under the name and address of the applicant to confirm the number. The above assertions are reviewed through an automated process, manual review of supporting documentation and reference to third party official databases. CPS section 4.2.2, PositiveSSL / PositiveSSL Wildcard / PositiveSSL Trial / OptimumSSL / OptimumSSL Wildcard / Comodo Multi-Domain / Instant DV SSL / Instant DV SSL Wildcard / Instant DV SSL Trial / Intel Pro SSL / Unified Communications / ComodoSSL: To validate these secure server certificates, Comodo checks that the Subscriber has control over the Domain name at the time the Subscriber submitted its enrollment certificates by reviewing the application information provided by the applicant (as per Section 4.3 of this CPS); and 1. Reviewing domain name ownership records publicly available through Internet approved global domain registrars and using generic e-mails which ordinarily are only available to person(s) controlling the domain name administration, for example, webmaster@ . . ., postmaster@ . . ., admin@; or 2. Requesting documentation that verifies control of the domain. In addition, Comodo at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement. CPS section 4.2.3, InstantSSL / Trial SSL / Content Verification Certificates: Comodo operates a website identity assurance database referred to as IdAuthority. The database contains pre-validated identification records for known domain names and uses automated algorithms to marry domain name ownership records (from global domain name registrars) with company ownership identification records (from official

	government and third party company information sources). If IdAuthority contains sufficient pre-validated records for the domain name used in an application, Comodo may employ the data held by IdAuthority to expedite the validation process. If application data matches the records held by IdAuthority, manual validation intervention is not required. In the event that the application data does not match the prevalidated records, the application is processed manually by a Comodo validation officer in accordance with the two-step process outlined in section 4.2.1 of this CPS. CPS section 4.2.4, InstantSSL / ProSSL / PremiumSSL / PremiumSSL Wildcard / EliteSSL /GoldSSL / PlatinumSSL / PlatinumSSL Wildcard / PremiumSSL Legacy / PremiumSSL Legacy Wildcard / PlatinumSSL Legacy / PlatinumSSL Legacy Wildcard / PlatinumSSL SGC Legacy / PlatinumSSL SGC Legacy Wildcard / Comodo SGC SSL / Comodo SGC SSL Wildcard / Educational Certificate / IGTF Certificate: Comodo may employ the data held by IdAuthority to expedite the validation process. If application data matches the records held by IdAuthority, manual validation intervention is not required. In the event that the application data does not match the pre-validated records, the application is processed manually by a Comodo validation officer in accordance with the process outlined in section 4.2.1 of this CPS. EV CPS Section 4.2.5: Verification of Applicant's Domain Name
Code Signing Subscriber Verification Procedures	CPS section 4.2.1 (see above)
Email Address Verification Procedures	CPS section 4.2.6: The Personal Secure Email Certificate is persona non-validated. Comodo only validates the right for the applicant to use the submitted email address. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by Comodo. The login details are sent via email to the address submitted during the certificate application. Once logged into the online certificate collection facilities and prior to the installation of the Personal Secure Email Certificate, Comodo validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application process. If the automated challenge is successful, Comodo will release the digital certificate to the subscriber. CPS section 4.2.7: Corporate Secure Email Certificates are only available through the EPKI Manager and will only be issued to email addresses within approved domain names. The EPKI Manager Account Holder must first submit a domain name to Comodo and appropriate domain name ownership, or right to use a domain name, validation takes place in accordance with 4.2.1 of this CPS except that a domain authorization letter may be used in substitution of any domain ownership validation. Upon successful validation of a submitted domain name or receipt of domain authorization letter, Comodo allows the EPKI Manager Account Holder to utilize email addresses within the domain name. The EPKI Manager nominated administrator applies for Corporate Secure Email Certificates. The administrator will submit the secure email certificate end-entity information on behalf of the end- entity. An email is then delivered to the end-entity containing unique login details to online certificate generation and collection facilities hosted by Comodo.

	Once logged into the online certificate generation and collection facilities, the end-entity's browser creates a public and private key pair. The public key is submitted to Comodo who will issue a Corporate Secure Email Certificate containing the public key. Comodo then validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during this automated application process. If the automated challenge is successful, Comodo will release the digital certificate to the end-entity subscriber.
Multi-factor Authentication	CPS section 1.10.1: For the issuance of Secure Server Certificates this Registration Authority is also equipped with automated systems that validate domain control. For that minority of secure server certificates for which domain control is not possible by completely automated means, the specially trained and vetted staff that we employ in our Registration Authority have the ability to cause the issuance of certificates – but only when they are authenticated to our issuance systems using true two-factor authentication.
Technical Constraints on Third-party Issuers	Please describe how it is ensured that only an internal Comodo RA does the domain control validation? i.e. Is it through the "Management Area" where RAs and Resellers are limited to what information they can verify? And then the "Management Area" requires a separate (Comodo automated or manual) approval of the domain name before the certificate request can be completed? CPS section 1.10: Only Registration Authorities which hold their own WebTrust for CAs Certification may issue or cause the issuance of SSL certificates. Other Registration Authorities may be enabled to perform validation of some or all of the subject identity information, but are not able to undertake domain control validation.
Network Security	Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Response to Mozilla's CA Recommended Practices (https://wiki.mozilla.org/CA:Recommended_Practices)

Publicly Available CP and CPS	See above.
CA Hierarchy	See above.
Audit Criteria	See above.
Document Handling of IDNs in CP/CPS	???
Revocation of Compromised Certificates	CPS section 4.13
Verifying Domain Name Ownership	See above.
Verifying Email Address Control	See above.
Verifying Identity of Code Signing Certificate Subscriber	See above.
DNS names go in SAN	???
Domain owned by a Natural Person	???
OCSP	See above.

Response to Mozilla's list of Potentially Problematic Practices (https://wiki.mozilla.org/CA:Problematic_Practices)

Long-lived DV certificates	Comodo issues DV certificates valid for up to 60 months. From 1st April 2015 Comodo will issue DV certificates for up to 39 months. This matches the requirement of section 9.4.1 of the CABF BRs.

	CPS section 4.8: Comodo verifies all information that is included in SSL certificates at time intervals of thirty-nine months or less. For unrevoked SSL certificates valid for more than 39 months, Comodo verifies that all of the information that is included in SSL certificates remains current and correct at time intervals of thirty-nine months or less.
Wildcard DV SSL certificates	Comodo issues Wildcard DV certificates and Wildcard OV certificates. CPS section 4.2.2: To validate these secure server certificates, Comodo checks that the Subscriber has control over the Domain name at the time the Subscriber submitted its enrollment certificates by reviewing the application information provided by the applicant (as per Section 4.3 of this CPS); and 1. Reviewing domain name ownership records publicly available through Internet approved global domain registrars and using generic e-mails which ordinarily are only available to person(s) controlling the domain name administration, for example, webmaster@ . . ., postmaster@ . . ., admin@; or 2. Requesting documentation that verifies control of the domain. In addition, Comodo at its discretion may establish domain control by utilizing third party domain name registrars and directories, by verifying control of the domain by practical demonstration of the control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.
Email Address Prefixes for DV Certs	When validating domain control using an email challenge-response, Comodo permit the use of the following email address prefixes when used with the domain for which the certificate is being requested. admin@ administrator@ hostmaster@ postmaster@ webmaster@ In addition we accept the use of an email address found in the WHOIS record of the domain for which the certificate is being requested.
Delegation of Domain / Email validation to third parties	In the general case, Comodo does not delegate Email validation to third parties, although there are some third parties which are able to issue email certificates for anything@domain.com where there is a per third-party whitelist of possible values of domain.com. (CPS section 4.2.7) Comodo does not delegate Domain validation to third parties – unless they get a separate WebTrust audit? CPS section 1.10: "**Only Registration Authorities which hold their own WebTrust for CAs Certification may issue or cause the issuance of SSL certificates. Other Registration Authorities**

	may be enabled to perform validation of some or all of the subject identity information, but are not able to undertake domain control validation." CPS section 1.11.1: Comodo operates a Reseller Partner network that allows authorized partners to integrate Comodo digital certificates into their own product portfolios. Reseller Partners are responsible for referring digital certificate customers to Comodo, who maintain full control over the certificate lifecycle process, including application, issuance, renewal and revocation. CPS section 1.11.2: Comodo operates the Powered SSL service that includes an international network of approved organizations sharing the Comodo practices and policies and using a suitable brand name to issue privately labeled Secure Server Certificates to individuals and companies. Comodo controls all aspects of the certificate lifecycle, including but not limited to the validation, issuance, renewal and revocation of Powered SSL certificates, however issued certificates contain an amended certificate profile to reflect the Powered SSL status to relying parties (ultimately customers).
Issuing end entity certificates directly from roots	Comodo does not issue end entity certificates directly from root CAs.
Allowing external entities to operate subordinate CAs	Where Comodo issues subordinate CA certificates to external entities they are either technically constrained or publicly disclosed and audited as per Mozilla's Inclusion Policy.
Distributing generated private keys in PKCS#12 files	Comodo does not generate key-pairs for end entity SSL certificates. In the general case for client certificates (including SMIME) Comodo does not generate key-pairs for end entity client certificates. In specific enterprise and academic environments where key backup and/or key escrow are supported for client encryption certificates we do generate the key-pair for the end-entity certificates but we do not transfer certificates with their keys through unsecure electronic channels.
Certificates referencing hostnames or private IP addresses	We follow the CABF Baseline Requirements, including the date restrictions on the issuance of certificates including a Reserved IP Address or Internal Server Name in BR section 9.2.1.
Issuing SSL Certificates for Internal Domains	We recognize .int as an internet-resolvable TLD. We operate a process to incorporate new TLDs as they are registered by ICANN.
OCSP Responses signed by a certificate under a different root	Comodo does not sign OCSP Responses using a certificate under a different root.
CRL with critical CIDP Extension	Comodo does not issue partitioned or partial CRLs.
Generic names for CAs	Two of the roots in this request have: "O = The USERTRUST Network", and nothing in the Issuer field to indicate that Comodo owns the root. Please explain why this "O" is meaningful. Is there actually a registered organization and/or trademark named "The USERTRUST Network"?
Lack of Communication With End Users	Comodo undertakes to continue to respond to end user concerns.