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.	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.	This "USERTrust ECC Certification Authority" root certificate is the ECC version of the "USERTrust RSA Certification Authority" root certificate.
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 - COMODO RSA Code Signing 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 are also planned: - USERTrust RSA Client Authentication and	“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 are also planned: - USERTrust ECC Client Authentication and

	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.	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.	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. There are no currently externally-operated subCAs under the “COMODO Certification Authority” root certificate that will be transitioned to this new root.	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. Regarding externally-operated subCAs issued from any of our existing roots and their potential transition to these new roots: previously, externally operated subCAs have (where not already compliant with v2.1 of Mozilla's policy) 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 See current versions of the CPS, EV SSL CPS, Addendum to EV SSL CPS, and ECC addendum to EV SSL CPS.
Audits	Auditor: Ernst & Young WebTrust CA audit statement: https://cert.webtrust.org/SealFile?seal=1613&file=pdf (2013.12.06) WebTrust EV audit statement: https://cert.webtrust.org/SealFile?seal=1614&file=pdf (2013.12.06) BR Audit Statement: https://cert.webtrust.org/SealFile?seal=1644&file=pdf (2014.02.03)
Baseline Requirements (SSL)	CPS section 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	CPS section 3.2.2 and EV SSL CPS section 4.2
DV SSL Verification	CPS section 3.2.2.1: For each domain name to be included in the SSL certificate Subject, Comodo verifies the Applicants control of the domain name in accordance with the CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as follows; 1. Confirming the Applicant as the Domain Name Registrant directly with the Domain Name Registrar; 2. Communicating directly with the Domain Name Registrant using an address, email, or telephone number provided by the Domain Name Registrar; 3. Communicating directly with the Domain Name Registrant using an email address created by pre-pending 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' in the local part, followed by the at-sign ("@"), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN; 4. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the FQDN, or; 5. Having the Applicant demonstrate practical control over the FQDN by making an agreed-upon change to information found in the DNS containing the FQDN;
OV SSL Verification	CPS section 3.2.2.2
EV SSL Verification	CPS section 3.2.2.3 EV CPS Section 4.2.5: Verification of Applicant's Domain Name
Code Signing Subscriber Verification	CPS sections 3.2.2.2, 3.2.2.3, 3.2.3.2
Email Address Verification	CPS section 3.2.5.1, S/MIME / Client Certificates: The request is verified via email sent to the email address to be contained in the Certificate Subject CPS section 3.2.7.1, Personal Secure Email Certificate: The only identifying information in the subject DN is the email address of the Subscriber. Comodo validates the right for the Applicant to use the submitted email address. This is achieved through the delivery via a challenge and response made to the email address submitted during the Certificate application.

	CPS section 3.2.7.2, Corporate Secure Email Certificate: 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 3.2.7.1 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. CPS section 3.2.7.5, Personal Authentication Certificates: Personal Authentication Certificates always contain an email address. Comodo validates the right for the Applicant to use the submitted email address. This is achieved through the delivery of a challenge and response made to the email address submitted during the Certificate application.
Multi-factor Authentication	CPS section 1.3.2.1: For the issuance of Secure Server Certificates this RA is also equipped with automated systems that validate domain control. For that minority of Secure Server Certificates for which the validation of domain control is not possible by completely automated means, the specially trained and vetted staff that Comodo employs in its RA have the ability to cause the issuance of Certificates – but only when they are authenticated to Comodo's issuance systems using two factor authentication. CPS section 1.3.2: RAs may only undertake their validation duties from pre-approved systems which are identified to the CA by various means that always include but are not limited to the white-listing of the IP address from which the RA operates.
Technical Constraints on Third-party Issuers	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? Comment #16: Yes, RAs & resellers (& any other type of account holder other than an internal Comodo RA account) are not able to give any indication about whether or not DCV has been completed. Server certificate requests placed with us always, without exception, hold until the domain name has been approved following either a Comodo-automated domain control validation or a manual approval given by an authorized Comodo internal RA operator. CPS section 1.3.2: Only RAs which hold their own WebTrust for CAs Certification may issue or cause the issuance of SSL Certificates. Other RAs 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	Comment #16: We confirm that we 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	Comment #16: The next revision of our CPS will document our handling of IDNs. Every certificate request that includes one or more IDNs is flagged for manual review by an internal Comodo RA operator.
Revocation of Compromised Certificates	CPS section 4.9
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	Comment #16: Comodo follows the BRs (9.2.1 and 9.2.2) in our inclusion of DNS names in SANs.
Domain owned by a Natural Person	Comment #16: When we issue a server certificate to an individual we put the person's name into the 'O' field of the certificate subject.
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. CPS section 6.3.2: Comodo verifies all information that is included in SSL certificates at time intervals of thirty-nine months or less.
Wildcard DV SSL certificates	Comodo issues Wildcard DV certificates and Wildcard OV certificates. CPS section 3.2.2.1: domain control validation for DV SSL certs CPS section 3.2.2.2: organization validation in addition to domain control validation.
Email Address Prefixes for DV Certs	CPS section 3.2.2.1: Communicating directly with the Domain Name Registrant using an email address created by pre-pending ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, or ‘postmaster’ in the local part, followed by the at-sign (“@”), followed by the Domain Name, which may be formed by pruning zero or more components from the requested FQDN;
Delegation of Domain / Email validation to third parties	CPS section 1.3.2.2 Web Host Resellers CPS section 1.3.2.3 EPKI Manager Accounts CPS section 1.3.2.2: Web Host Resellers do not validate domain control for Secure Server Certificates. This element of the validation of Secure Server Certificates is always performed by Comodo’s internal RA as described in 1.3.2.1. 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 3.2.7.2)

	CPS section 1.3.2: “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.” Comment #16: This was a statement introduced to implement and formalize our acceptance of Microsoft's requirement of us in their amendment to their CA program technical requirements dated April 6, 2011, that "3. Resellers and Registration Authorities (RAs) may not cause the issuance of certificates on behalf of a Program CA. a). For purposes of the Program, a reseller or RA that can cause the issuance of certificates on behalf of a Program CA is in fact a sub-CA of the Program CA, and will be treated as an extension of the CA, and is subject to the same terms and conditions as the Program CA, including audit requirements by a qualified audit authority.". It is a forward-looking statement since we do not have any external RAs who have their own WebTrust audits and if we did we would include the interface between our systems and theirs within the scope of our respective WebTrust audits.
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. Comment #16: "USERTrust" and "The USERTRUST Network" are names that Comodo has used since its purchase of Usertrust Inc. assets in 2004. We are carrying forward the use of this brand for the time being and we have trademark rights with respect to "USERtrust".
Lack of Communication With End Users	Comodo undertakes to continue to respond to end user concerns.