**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 comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

| **General Information** | **Data** |
|---|---|
| CA Name | COMODO |
| Website URL | http://www.comodo.com |
| Organizational type | Private Corporation |
| Primary market / customer base | Comodo CA Ltd is a commercial CA based in the UK and serving customers worldwide. |
| CA Contact Information | CA Email Alias: root.certificates@comodo.com<br>CA Phone Number: 44 161 874 7070<br>Title / Department: CA Technical |

COMODO is requesting inclusion of 3 new root certificates as follows.

**Certificate Name:** COMODO RSA Certification Authority
Cert Summary: Is this the next version of the "COMODO Certification Authority" root certificate that was included in bug #401587?
Certificate URL: http://crt.comodoca.com/COMODORSACertificationAuthority.crt
Version: X.509v3
SHA1 Fingerprint: AF:E5:D2:44:A8:D1:19:42:30:FF:47:9F:E2:F8:97:BB:CD:7A:8C:B4
Key Length: 4096-bit RSA
Valid From: 2010-01-19
Valid To: 2038-01-18
CRL URL: http://crl.comodoca.com/COMODORSACertificationAuthority.crl
OCSP URL: http://ocsp.comodoca.com
Test URL: https://comodorsacertificationauthority-ev.comodoca.com
CA Hierarchy: Please provide a description and/or diagram of the CA hierarchy that is planned for this root.
Externally operated subCAs: Does or will this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing: List any other root CAs that have (or are planned to) issued cross-signing certificates for this root CA.

**Certificate Name:** USERTrust RSA Certification Authority
Cert Summary: Is this the next version of one or more of the root certificates that were included in bug #242610?
Certificate URL: http://crt.usertrust.com/USERTrustRSACertificationAuthority.crt
Version: X.509v3
SHA1 Fingerprint: 2B:8F:1B:57:33:0D:BB:A2:D0:7A:6C:51:F7:0E:E9:0D:DA:B9:AD:8E
Key Length: 4096-bit RSA
Valid From: 2010-02-01
Valid To: 2038-01-18
CRL URL: http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
OCSP URL: http://ocsp.usertrust.com
Test URL: https://usertrustrsacertificationauthority-ev.comodoca.com
CA Hierarchy: Please provide a description and/or diagram of the CA hierarchy that is planned for this root.
Externally operated subCAs: Does or will this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing: List any other root CAs that have (or are planned to) issued cross-signing certificates for this root CA.

**Certificate Name:** USERTrust ECC Certification Authority
Cert Summary: Is this the next version of one or more of the root certificates that were included in bug #242610?
Certificate URL: http://crt.usertrust.com/USERTrustECCCertificationAuthority.crt
Version: X.509v3
SHA1 Fingerprint: D1:CB:CA:5D:B2:D5:2A:7F:69:3B:67:4D:E5:F0:5A:1D:0C:95:7D:F0
Key Length: SECG elliptic curve secp384r1 (aka NIST P-384)
Valid From: 2010-02-01
Valid To: 2038-01-18
CRL URL: http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl
OCSP URL: http://ocsp.usertrust.com
Test URL: https://usertrustecccertificationauthority-ev.comodoca.com
CA Hierarchy: Please provide a description and/or diagram of the CA hierarchy that is planned for this root.
Externally operated subCAs: Does or will this root have any subordinate CAs that are operated by external third parties? If yes, please see https://wiki.mozilla.org/CA:SubordinateCA_checklist
Cross-Signing: List any other root CAs that have (or are planned to) issued cross-signing certificates for this root CA.

The following information is common to all 3 of these root certificates.

| **Info Needed** | **Data** |
|---|---|
| CRL Update Frequency | CPS Section 3.7: Comodo CRLs for end-entity certs are valid for 24 hours. |
| OCSP Responder max expiration | What is the maximum expiration time for OCSP responses?<br>http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf Section 26(b): “If the CA provides revocation information |

| | |
|---|---|
| | via an Online Certificate Status Protocol (OCSP) service, it MUST update that service at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.” |
| Requested Trust Bits | Websites (SSL/TLS)<br>Email (S/MIME)<br>Code Signing |
| SSL Validation Type | DV, OV, and EV |
| If DV – email addresses used for verification | From CPS Section 4.2.2: “… for example, webmaster@ . . ., postmaster@ . . ., admin@; “<br>Are these the only email address prefixes that are allowed? If not, please provide the complete list of email address prefixes that Comodo uses, and where this is documented.<br>Please see: https://wiki.mozilla.org/CA:Problematic_Practices#Email_Address_Prefixes_for_DV_Certs |
| EV policy OID(s) | 1.3.6.1.4.1.6449.1.2.1.5.1 |
| CP/CPS | All documents are in English.<br>Repository: http://www.comodo.com/about/comodo-agreements.php<br>CPS: http://www.comodo.com/repository/09_22_2006_Certification_Practice_Statement_v.3.0.pdf<br>Will the CPS be updated in regards to these new roots? Or will there be an addendum to cover them?<br>EV CPS: http://www.comodo.com/repository/EV_CPS_4_JUN_07.pdf<br>EV Addendum to CPS: http://www.comodo.com/repository/EV_CPS_Amendment-June_2009.pdf<br>ECC CPS: http://www.comodo.com/repository/ECC_addendum_to_the_EV_Certification_Practice_Statement.pdf |
| AUDIT | Audit Type: WebTrust CA<br>Auditor: Ernst & Young, www.ey.com<br>Audit Reports and Management’s Assertions: https://cert.webtrust.org/ViewSeal?id=1082 (2010.03.31)<br>The currently included roots and all three of these new root certificates are included.<br><br>Audit Type: WebTrust EV<br>Auditor: Ernst & Young, www.ey.com<br>Audit Reports and Management’s Assertions: https://cert.webtrust.org/ViewSeal?id=1083 (2010.03.31)<br>“…for the ‘Comodo EV SGC SSL Certificate’ and ‘Comodo EV SSL Certificate’ products…”<br>How does, or will this relate to these new roots? |
| Organization Identity Verification | CPS section 4.2.1: “This process involves Comodo, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) in order to check that: …<br>2. The applicant is an accountable legal entity, whether an organization or an individual.<br>• Validated by requesting official company documentation, such as Business License, Articles of Incorporation, Sales License or other relevant documents.<br>• For non-corporate applications, documentation such as bank statement, copy of passport, copy of driving license or other relevant documents.<br>The above assertions are reviewed through an automated process, manual review of supporting documentation and reference to third party official databases.” |

| | |
|---|---|
| | EV CPS Section 4.2.1: Verification of Applicant’s Legal Existence and Identity<br>EV CPS Section 4.2.2: Verification of Applicant’s Legal Existence and Identity – Assumed Name<br>EV CPS Section 4.2.3: Verification of Applicant’s Physical Existence<br>EV CPS Section 4.2.4: Verification of Applicant’s Operational Existence |
| Domain Name Ownership / Control | EV CPS Section 4.2.5: Verification of Applicant’s Domain Name<br><br>CPS section 4.2.1: “This process involves Comodo, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) in order to check that:<br>1. The applicant has the right to use the domain name used in the application.<br>• Validated by reviewing domain name ownership records available publicly through Internet or approved global domain name registrars.<br>• Validation may be supplemented through the use of the administrator contact associated with the domain name register record for communication with Comodo validation staff or for automated email challenges.<br>• Validation may be supplemented through the use of generic emails which ordinarily are only available to the person(s) controlling the domain name administration, for example webmaster@..., postmaster@..., admin@...”<br><br>CPS section 4.2.2: “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<br>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<br>2. Requesting documentation that verifies control of the domain.” |
| Email Address Ownership / Control | CPS Section 4.2.6, Personal Secure Email Certificate: “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.”<br><br>CPS Section 4.2.7, Corporate Secure Email Certificate: “…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. Upon successful validation of a submitted domain name Comodo allows the EPKI Manager Account Holder to utilize email addresses within the domain name.” |
| Identity of Code Signing Subscriber | CPS section 4.2.8: “Code Signing Certificates and Time Stamping Certificates are processed by a Comodo validation officer in accordance with the process outlined in section 4.2.1 of this CPS. 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.” |
| Potentially Problematic Practices | Please review the list of Potentially Problematic Practices (http://wiki.mozilla.org/CA:Problematic_Practices). Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information.<br>• 1.1 Long-lived DV certificates<br>○<br>• 1.2 Wildcard DV SSL certificates<br>○<br>• 1.3 Email Address Prefixes for DV Certs<br>○<br>• 1.4 Delegation of Domain / Email validation to third parties<br>○<br>• 1.5 Issuing end entity certificates directly from roots<br>○<br>• 1.6 Allowing external entities to operate subordinate CAs<br>○<br>• 1.7 Distributing generated private keys in PKCS#12 files<br>○<br>• 1.8 Certificates referencing hostnames or private IP addresses<br>○<br>• 1.9 Issuing SSL Certificates for Internal Domains<br>○<br>• 1.10 OCSP Responses signed by a certificate under a different root<br>○<br>• 1.11 CRL with critical CIDP Extension<br>○<br>• 1.12 Generic names for CAs<br>○<br>• 1.13 Lack of Communication With End Users<br>○ |