Bugzilla ID: 926541
Bugzilla Summary: QuoVadis G3 (SHA256) Root Inclusion Request

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	QuoVadis Limited
Website URL	www.quovadisglobal.com
Organizational type	Commercial CA, operated by a private company.
Primark Market / Customer Base	QuoVadis is a commercial CA serving a global client base, active in both the markets for SSL and End User certificates with a focus on digital signatures. The company is a Qualified Certification Services Provider in Switzerland and Holland, and an issuer in the SuisseID (CH) and PKI Overheid (NL) eID programmes. QuoVadis serves both enterprises and individuals.
Impact to Mozilla Users	The QuoVadis G3 (SHA256) Root Certificates will eventually replace the existing QuoVadis Root Certificates that are distributed in NSS (see bugs 378161 and 365281).
Inclusion in other major browsers	Yes, the QuoVadis Root Certificates are widely distributed.
CA Contact Information	CA Email Alias: compliance@quovadisglobal.com CA Phone Number: 1-441-278-2803 Title / Department: QuoVadis Policy Management Authority (PMA)

Technical information about each root certificate

Certificate Name	QuoVadis Root CA 1 G3	QuoVadis Root CA 2 G3	QuoVadis Root CA 3 G3
Certificate Issuer Field	CN = QuoVadis Root CA 1 G3 O = QuoVadis Limited C = BM	CN = QuoVadis Root CA 2 G3 O = QuoVadis Limited C = BM	CN = QuoVadis Root CA 3 G3 O = QuoVadis Limited C = BM
Certificate Summary	This SHA256 will eventually replace the "QuoVadis Root Certification Authority" Root Certificate that is currently included in NSS.	This SHA256 will eventually replace the "QuoVadis Root CA 2" Root Certificate that is currently included in NSS.	This SHA256 will eventually replace the "QuoVadis Root CA 3" Root Certificate that is currently included in NSS.
Root Cert URL	http://trust.quovadisglobal.com/qvrca1g3.crt	http://trust.quovadisglobal.com/qvrca2g3.crt	http://trust.quovadisglobal.com/qvrca3g3.crt
SHA1 Fingerprint	1B:8E:EA:57:96:29:1A:C9:39:EA:B8:0A:81:1A:73:73:C0:93:79:67	09:3C:61:F3:8B:8B:DC:7D:55:DF:75:38:02:05:00:E1:25:F5:C8:36	48:12:BD:92:3C:A8:C4:39:06:E7:30:6D:27:96:E6:A4:CF:22:2E:7D
Valid From	2012-01-12	2012-01-12	2012-01-12
Valid To	2042-01-12	2042-01-12	2042-01-12

Certificate Version	3	3	3
Certificate Signature Algorithm	sha256RSA	sha256RSA	sha256RSA
Signing key parameters	4096	4096	4096
Test Website URL (SSL) Example Certificate (non---SSL)	Valid: https://qvica1g3-v.quovadisglobal.com Additional test certificates (expired, revoked) at http://www.quovadisglobal.com/en-GB/QVRepository/TestCertificates.aspx	Valid: https://qvsslicag3-v.quovadisglobal.com (EV) https://evsslicag3-v.quovadisglobal.com Additional test certificates (expired, revoked) at http://www.quovadisglobal.com/en-GB/QVRepository/TestCertificates.aspx	Valid: https://qvica3g3-v.quovadisglobal.com Additional test certificates (expired, revoked) at http://www.quovadisglobal.com/en-GB/QVRepository/TestCertificates.aspx
CRL URL	http://crl.quovadisglobal.com/qvrca1g3.crl	http://crl.quovadisglobal.com/qvrca2g3.crl	http://crl.quovadisglobal.com/qvrca3g3.crl
OCSP URL (Required now)	http://ocsp.quovadisglobal.com	http://ocsp.quovadisglobal.com	http://ocsp.quovadisglobal.com
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	OV	OV, EV	OV
EV Policy OID(s)	NA	1.3.6.1.4.1.8024.0.2.100.1.2 EV Tested: https://bugzilla.mozilla.org/attachment.cgi?id=818588	NA

CA Hierarchy information for each root certificate

CA Hierarchy	Each root will sign at least one subordinate CA for issuing end-entity certificates. At this time we expect <the hierarchy under the G3 roots> will be very similar to the hierarchy of the current roots.
Externally Operated SubCAs	The CP/CPS for QuoVadis Root CA1 and Root CA3 section 1.3.1.5 allows for subCAs that are operated by external third parties (aka "Approved Client Issuing CAs"). In the past, these private subCAs have been overseen via contractual controls or technical monitoring, supported by internal audit. QuoVadis is in the process of transitioning these clients to either technical controls (nameConstraints) or audit with public disclosure as specified in Section 9 of the Mozilla CA Inclusion Policy. Any external SubCAs added to the G3 hierarchy will comply with that Section 9 of the Mozilla CA Inclusion Policy from inception.
Cross-Signing	At present, we do not expect to have any cross-certificates for the QuoVadis G3 Root Certificates. However, if we need to start using the G3 Roots before they have achieved a sufficient level of distribution amongst the installed base of various software products, we may elect to issue cross-certificates to the new Roots from the existing QuoVadis Roots.

Verification Policies and Practices

Policy Documentation	All Documents are in English. QuoVadis Document Repository: https://www.quovadisglobal.com/QVRepository.aspx QuoVadis Root CA1 and QuoVadis Root CA3 share a CP/CPS (covering both G1 and G3): https://www.quovadisglobal.com/~/media/Files/Repository/QV_RCA1_RCA3_CPCPS_V4_13.ashx QuoVadis Root CA2 has its own CP/CPS covering both G1 and G3: https://www.quovadisglobal.com/~/media/Files/Repository/QV_RCA2_CPCPS_v1.13.ashx QuoVadis Relying Party Agreement: https://www.quovadisglobal.com/~/media/Files/Repository/QV_RPA_v1%201.ashx QuoVadis Certificate Holder Agreement: https://www.quovadisglobal.com/~/media/Files/Repository/QV_Cert_Holder_v1_2.ashx QuoVadis Code Signing Subscriber Agreement: https://www.quovadisglobal.com/~/media/Files/Repository/QV_SA_Code_v1_1.ashx
Audits	Audit Type: WebTrust Auditor: Ernst & Young Auditor Website: http://www.ey.com URL to Audit Report and Management's Assertions: • WebTrust for CAs: https://cert.webtrust.org/SealFile?seal=1503&file=pdf (2013.05.31) • WebTrust for Extended Validation: https://cert.webtrust.org/SealFile?seal=1508&file=pdf • WebTrust for Baseline Requirements: https://cert.webtrust.org/SealFile?seal=1520&file=pdf Ernst & Young auditors were present for the creation ceremony for the G3 Roots. QuoVadis undergoes additional external audits for standards including ETSI TS 101.445 with KPMG. For more information see: http://www.quovadisglobal.com/AboutUs/Accreditations.aspx
Baseline Requirements (SSL)	Section 1.1 of both CP/CPS documents. The current WebTrust reports include the G3 Roots.
SSL Verification Procedures	QuoVadis SSL verification procedures for Business SSL (OV) and EV SSL are in Appendix B of the CP/CPS for Root CA2. QuoVadis SSL verification procedures for Business SSL (OV) are in Section 10.7 of the CP/CPS for QuoVadis Root CA1 and Root CA3. Of note, QuoVadis primarily serves the enterprise market with managed PKI offerings (rather than retail), allowing greater control over the validation process via pre-authorised personnel at the customer. Domain validation is performed manually, typically based on information from WHOIS. When challenge response emails are used, the addresses include the WHOIS contacts, admin@, administrator@, webmaster@, hostmaster@, and postmaster@.

	QuoVadis maintains automatic blocks in our issuing systems for high-profile domain names. These requests must be approved by a QuoVadis Administrator with a higher role than involved in frontline Support.
Organization Verification Procedures	See above. QuoVadis issues OV and EV certificates, and the accuracy of information in the Subject DN is validated using external data sources.
Email Address Verification Procedures	End user certificates are issued via our Trust/Link system. A user is "invited" by an administrator via a system-generated email to the address that will be in the certificate (along with an out-of-band shared secret for the user to accept the invitation). Before the certificate is created, the user creates their own password (known only to them) which is used for future key/certificate management activity.
Code Signing Subscriber Verification Procedures	QuoVadis verification procedures for code signing certificates are in Appendix B of the CP/CPS for Root CA2, and in 10.7 of the CP/CPS for QuoVadis Root CA1 and Root CA3.
Multi-factor Authentication	Multi-factor authentication (smartcard) is required for all accounts capable of directly causing certificate issuance.
Network Security	QuoVadis confirms the following: • Maintain network security controls that at minimum meet the CA/B Forum Network and Certificate System Security Requirements. • Check for mis-issuance of certificates, especially for high-profile domains. • Review network infrastructure, monitoring, passwords, etc. for signs of intrusion or weakness. • Ensure Intrusion Detection System and other monitoring software is up-to-date. • Able to shut down certificate issuance quickly if we are alerted of intrusion.

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

Publicly Available CP and CPS	Yes
CA Hierarchy	Yes
Audit Criteria	Yes, WebTrust, see above.
Document Handling of IDNs in CP/CPS	IDN certificates are not issued.
Revocation of Compromised Certificates	Yes, see Section 4.9.1 of both CP/CPS documents.
Verifying Domain Name Ownership	Yes, see above.
Verifying Email Address Control	Yes, see above.
Verifying Identity of Code Signing Certificate Subscriber	Yes, see above.
DNS names go in SAN	Yes
Domain owned by a Natural Person	No
OCSP	Yes

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

Long-lived DV certificates	NA. SSL certificates are OV or EV. SSL validity periods comply with the Baseline Requirements and EV Guidelines as appropriate.
Wildcard DV SSL certificates	NA
Email Address Prefixes for DV Certs	NA
Delegation of Domain / Email validation to third parties	Domain and Email validation are performed by QuoVadis.

Issuing end entity certificates directly from roots	NA – QuoVadis always issues from an intermediate Issuing CA.
Allowing external entities to operate subordinate CAs	See above. External subCAs added to the G3 hierarchy will comply with Section 9 of the Mozilla CA Inclusion Policy from inception.
Distributing generated private keys in PKCS#12 files	QuoVadis does not generate key pairs for SSL and signing certificates. Certain QuoVadis end user certificate policies (such as those for S/MIME) at customer's request allow QuoVadis to generate key pairs and optionally to archive. See section 10.1.2 of the CP/CPS for Root CA1/Root CA3. Our issuance process allows the Certificate Holder to select their own password in an out of band process (unknown to Administrators). That password is used to encrypt the .p12 file for delivery. In the case of archive, if a certificate/private key is retrieved by anyone other than the Certificate Holder (ie an authorized Administrator), the certificate is simultaneously revoked and the Certificate Holder is notified.
Certificates referencing hostnames or private IP addresses	QuoVadis has issued OV SSL (never EV) referencing internal server names, and has implemented procedures to deprecate their use in line with the Baseline Requirements. See Section 3.1.1 of the CP/CPS for Root CA2. QuoVadis communicates the risks of such practices with customers, and such requests are approved by a QuoVadis Administrator before issuance. QuoVadis will not issue SSL including internal server names with an Expiry Date later than November 1, 2015. Effective 1 October 2016, QuoVadis will revoke any unexpired SSL whose CN or SAN contains internal server names.
Issuing SSL Certificates for Internal Domains	Yes. QuoVadis SSL issuance systems filter against an internal database of approved TLDs that are eligible to be used for domains in certificates, and that list is manually updated. The system also alerts when certificates are issued using high risk domains.
OCSP Responses signed by a certificate under a different root	OCSP signing certificates are issued by the CA served by the OCSP.
CRL with critical CIDP Extension	QuoVadis CRL CIDP are not marked critical.
Generic names for CAs	QuoVadis uses meaningful CN and OU in its CA certificates.
Lack of Communication With End Users	QuoVadis is contactable on policy related issues at compliance@quovadisglobal.com. In addition, our websites include contact forms as well as certificate problem reporting and revocation request forms that are routed to the appropriate Support teams for prompt action.