Bugzilla ID: 636557
Bugzilla Summary: Add Visa Information Delivery Root CA certificate

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	Visa
Website URL	http://www.visa.com
Organizational type	Private Corporation
Primark Market / Customer Base	Financial services, Global
Impact to Mozilla Users	The inclusion of this certificate authority will enable Mozilla's consumers to authenticate to Visa products and services. Root inclusion will affect any Visa issuing bank using any of Visa's secured web based services. Certificates used by this CA will be used to support payment and information delivery applications (business to business payments, business to consumer payments, non-payment applications) as well as some Visa internal applications. All of these applications are tied to Visa products, services or platforms that are governed by Visa's global operating regulations that bind all of the parties to specified terms, conditions, responsibilities, recourse, etc. Given our large international participation base -- 21,000+ banks, billions of customers, millions of acceptors and our global nature -- warrants the use of the Root CA infrastructure that is owned and managed by Visa.
CA Contact Information	CA Email Alias: PKIPolicy@visa.com, mstefani@visa.com, rburgos@visa.com CA Phone Number: (303) 389-7750 Title / Department: Cryptographic Review Forum (CRF)

Technical information about each root certificate

Certificate Name	Visa Information Delivery Root CA
Certificate Issuer Field	CN = Visa Information Delivery Root CA OU = Visa International Service Association O = VISA C = US
Certificate Summary	This root has several internally-operated subordinate online CAs that issue end entity certificates for SSL client, SSL server, digital signature, VPN/IP Sec, SSL Server & Client.
Root Cert URL	http://enroll.visaca.com/VisaInfoDeliveryRootCA.crt
SHA1 Fingerprint	5A:4D:0E:8B:5F:DC:FD:F6:4E:72:99:A3:6C:06:0D:B2:22:CA:78:E4
Valid From	2005-06-27
Valid To	2025-06-29
Certificate Version	3

Cert Signature Algorithm	sha1RSA
Signing key parameters	2048
Test Website URL (SSL)	Need an https url to a website whose SSL certificate chains up to this root. Please test in Firefox before providing.
CRL URL	http://enroll.visaca.com/VisaInfoDeliveryRootCA.crl When I try to import this CRL into my Firefox browser, I get the following error. Error Importing CRL to local Database. Error Code:ffffe009 • ffffe009 is equivalent to -8183, "Security library: improperly formatted DER-encoded message." It means that the reply contained anything other than a valid DER-encoded CRL. Typical Resolution: Change encoding from PEM to DER. Please correct and test with Firefox. Comment #7: For end-entity certificates under the issuing sub CA, VI CA1, nextUpdate is 5 days. For end-entity certificates under the issuing sub CA, VI CA2, nextUpdate is 2 days. For end-entity certificates under the issuing sub CA, VI CA3, nextUpdate is 7 days. For end-entity certificates under the issuing sub CA, VI CA4, nextUpdate is 3 days.
OCSP URL	None
Requested Trust Bits	Websites (SSL/TLS)
SSL Validation Type	OV
EV Policy OID(s)	Not EV

CA Hierarchy information for each root certificate

CA Hierarchy	The Visa Information Delivery Root CA which provides Certificate Signing, Off-line CRL Signing, CRL Signing; has several subordinate online CAs that issue end entity certificates (SSL client, SSL server, digital signature, VPN/IP Sec, SSL Server & Client). Email (S/MIME) and Code Signing Certificates ARE NOT issued from the Visa Information Delivery subordinate online CAs. This root has four internally-operated subordinate Issuing CAs that only issue end-entity certificates: (1) VICA1 – Visa Inc. Certificate Authority for Internet use (2) VICA2 – Visa Inc. Certificate Authority for Intranet use (3) Visa Inc. External Issuing Certificate Authority for Internet use – VI CA3 (4) Visa Inc. Internal Issuing Certificate Authority for Intranet use – VI CA4
Externally Operated SubCAs	None
Cross-Signing	None

Verification Policies and Practices

Policy Documentation	Visa PKI Disclosure Statement: http://www.visa.com/pki CP (English): https://partnernetwork.visa.com/vpn/global/retrieve_document.do?documentRetrievalId=100176 The CP uses the term "Visa InfoDelivery Root" to refer to this root.
Audits	Audit Type: WebTrust CA Auditor: KPMG Audit Report and Management's Assertions: https://bugzilla.mozilla.org/attachment.cgi?id=555751 (2010.05.31)

Organization Verification Procedures	CP section 3.3: The Certificate Authorities (CAs) or Registration Authorities (RAs) must verify the identity of the Subscriber and the Visa business relationship. … The RA has the responsibility, on behalf of a Certificate Authority (CA), for: 1. Verifying that all of the prerequisites that must be performed prior to the generation of the key pair and certificate request have been successfully completed 2. Authenticating the entity submitting the request in accordance with the identification and authentication procedures specified for the type of certificate and/or for the Visa product or service with which the certificate is intended to be used 3. Verifying that the certificate request has been transferred from the Subscriber to the RA in a secure manner as defined by the Visa CPS 4. Processing the certificate request, along with the appropriate documentation, to the Certificate Authority (CA) as defined by the Visa CPS … Authorization to request a certificate will be required to be an official appointment (for example, company/organization letter signed by an organizational authority).
SSL Verification Procedures	CP section 3.2: • The use of a domain name is restricted to the legal owner of that domain name. • The use of an email address is restricted to the legal owner of that email address. • The use of a registered name is restricted to the legal owner of that registered name.
Email Address Verification Procedures	Not applicable – Not requesting enablement of the email trust bit for this root.
Code Signing Subscriber Verification Procedures	Not applicable – Not requesting enablement of the code signing trust bit for this root.

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

Publicly Available CP and CPS	The CP is available on Visa's website.
CA Hierarchy	The root signs internally-operated intermediate certificates which sign end-entity certs.
Audit Criteria	Yes
Document Handling of IDNs in CP/CPS	CP section 3.2: Certificates that contain a domain name not owned by Visa ("foreign entity certificates"), for example, server_name.BankX.com., may be signed and requires signed written permission by an officer (Vice President level or above) on company letterhead from the company that owns the domain name authorizing the signing of the certificate.
Revocation of Compromised Certificates	CP Section 4.8: Certificate Revocation and Suspension
Verifying Domain Name Ownership	See above
Verifying Email Address Control	N/A
Verifying Identity of Code Signing Certificate Subscriber	N/A
DNS names go in SAN	Comment #8: We normally place primary DNS names within the SAN (Subject Alternate Name) extension of X.509v3 certificates and in some instances use the SCN (Subject Common Name) for the

	primary DNS name (This is dependent on the subject application's architectural requirements).
Domain owned by a Natural Person	Domain names owned by individuals are NOT permitted by VISA. (CP section 3.2)
OCSP	N/A

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

Long-lived DV certificates	SSL certs are OV.
Wildcard DV SSL certificates	SSL certs are OV. CP section 3.2: Certificates that contain wildcard characters ("wildcard certificates") may be signed with the following restrictions: - The naming convention of *.<application_name>.<visa_owned_domain_name>.com is used (for example, *.VOL.VISA.COM). - The application processes transactions at multiple geographic locations where "application session stickiness" is required (for example, active/active at multiple data centers). - No more than 30 servers shall use a single wildcard certificate.
Email Address Prefixes for DV Certs	If DV SSL certs, then list the acceptable email addresses that are used for verification.
Delegation of Domain / Email validation to third parties	No. CP section 1.3: A Certificate Authority (CA) PKI administrator must be an employee of Visa. … RA staff must be Visa employees or contractors.
Issuing end entity certificates directly from roots	No. Root signs intermediate CAs which sign end-entity certs.
Allowing external entities to operate subordinate CAs	Not allowed.
Distributing generated private keys in PKCS#12 files	N/A
Certificates referencing hostnames or private IP addresses	N/A
Issuing SSL Certificates for Internal Domains	CP section 3.2
OCSP Responses signed by a certificate under a different root	N/A
CRL with critical CIDP Extension	?
Generic names for CAs	CN not generic.
Lack of Communication With End Users	NA