Print this page

Mozilla - CA Program

Case Information

Case Number	00000050	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owners/Certificate Name	Visa	**Request Status**	Need Information from CA

Additional Case Information

Subject	New Owner/Root inclusion requested	**Case Reason**	New Owner/Root inclusion requested

Bugzilla Information

Link to Bugzilla Bug	https://bugzilla.mozilla.org /show_bug.cgi?id=636557

General information about CA's associated organization

Company Website	http://www.visa.com/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	Global	**Verified?**	Verified
Primary Market / Customer Base	Financial services	**Verified?**	Verified
Impact to Mozilla Users	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. Large international participation base: 21,000+ banks, billions of customers, millions of acceptors.	**Verified?**	Verified

Response to Mozilla's list of Recommended Practices

Recommended Practices	https://wiki.mozilla.org /CA:Recommended_Practices#CA_Recommended_Practices	**Recommended Practices Statement**	I have reviewed Mozilla's list of Recommended Practices, and confirm that we follow those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Recommended Practices	* 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	**Verified?**	Verified

owns the domain name authorizing the signing of the certificate.
* CP Section 4.8: Certificate Revocation and Suspension
* 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 names owned by individuals are NOT permitted by VISA. (CP section 3.2)

Response to Mozilla's list of Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA:Problematic_Practices#Potentially_problematic_CA_practices	**Problematic Practices Statement**	I have reviewed Mozilla's list of Potentially Problematic Practices, and confirm that we do not do those practices, with exceptions and clarifications noted in the text box below.
CA's Response to Problematic Practices	* 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. * CP section 1.3: A Certificate Authority (CA) PKI administrator must be an employee of Visa. … RA staff must be Visa employees or contractors. NEED: Please also respond to: https://wiki.mozilla.org/CA:Problematic_Practices#SHA-1_Certificates	**Verified?**	Need Response From CA

Root Case Record # 1

Root Case Information

Root Case No	R00000066	**Case Number**	00000050
Request Status	Need Information from CA	**Root Certificate Name**	Visa Information Delivery Root CA

Additional Root Case Information

Subject	Include Visa Information Delivery Root CA

Technical Information about Root Certificate

O From Issuer Field	VISA	**Verified?**	Verified
OU From Issuer Field	Visa International Service Association	**Verified?**	Verified

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.	**Verified?**	Verified
Root Certificate Download URL	http://enroll.visaca.com /VisaInfoDeliveryRootCA.crt	**Verified?**	Verified
Valid From	2005 Jun 27	**Verified?**	Verified
Valid To	2025 Jun 29	**Verified?**	Verified
Certificate Version		**Verified?**	Verified
Certificate Signature Algorithm	SHA-1	**Verified?**	Verified
Signing Key Parameters	2048	**Verified?**	Verified
Test Website URL (SSL) or Example Cert	https://enroll.visaca.com/	**Verified?**	Verified
CRL URL(s)	http://www.visa.com /pki/revocationlist.html http://Enroll.visaca.com/VICA3.crl http://Enroll.visaca.com /VisaInfoDeliveryRootCA.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.visa.com/ocsp	**Verified?**	Verified
Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
EV Policy OID(s)	Not requesting EV treatment	**Verified?**	Not Applicable
EV Tested		**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Digital Fingerprint Information

SHA-1 Fingerprint	5A:4D:0E:8B:5F:DC:FD:F6:4E:72:99:A3:6C:06:0D:B2:22:CA:78:E4	**Verified?**	Verified
SHA-256 Fingerprint	C5:7A:3A:CB:E8:C0:6B:A1:98:8A:83:48:5B:F3:26:F2:44:87:75:37:98:49:DE:01:CA:43:57:1A:F3:57:E7:4B	**Verified?**	Verified

CA Hierarchy Information

CA Hierarchy	CA Hierarchy Diagram in Figure 1-2 of the CP. 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	**Verified?**	Verified

Externally Operated SubCAs	None. CP section 1.1: With the exception of the Visa Smart Debit/Credit (VSDC) PKI, Certificate Authorities (CAs) certificates can only be issued to Visa or Visa Business Groups.	**Verified?**	Verified
Cross Signing	None. CP section 3.3: Cross certification within Certificate Authorities (CAs) or with external Certificate Authorities (CAs) ... is not supported. The Visa PKI hierarchy is a closed PKI.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CP section 1.3: A Certificate Authority (CA) PKI administrator must be an employee of Visa. … RA staff must be Visa employees or contractors.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English. The CP refers to this root as "Visa InfoDelivery Root"	**Verified?**	Verified
CA Document Repository	http://www.visa.com/pki	**Verified?**	Verified
CP Doc Language	English		
CP	http://www.visa.com/pki/pdf/VisaPublicKeyInfrastructureCertificatePolicy.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	Not published. See CP.	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable
Auditor Name	KMPG	**Verified?**	Verified
Auditor Website	http://www.kpmg.com/	**Verified?**	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	**Verified?**	Verified
Standard Audit	https://bug636557.bugzilla.mozilla.org/attachment.cgi?id=8475469	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	6/6/2014	**Verified?**	Verified
BR Audit	NEED: BR audit statement for this root and hierarchy. Please see: https://wiki.mozilla.org/CA:BaselineRequirements	**Verified?**	Need Response From CA
BR Audit Type		**Verified?**	Need Response From CA
BR Audit Statement Date		**Verified?**	Need Response From CA
EV Audit	Not requesting EV treatment.	**Verified?**	Not Applicable
EV Audit Type		**Verified?**	Not Applicable
EV Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	NEED: https://wiki.mozilla.org/CA:BaselineRequirements#CA_Conformance_to_the_BRs The CA's CP or CPS documents must include a commitment to comply with the BRs, as described in BR section 8.3.	**Verified?**	Need Response From CA

SSL Verification Procedures	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. 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. - 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.	**Verified?**	Verified
EV SSL Verification Procedures	Not requesting EV treatment for this root.	**Verified?**	Not Applicable
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).	**Verified?**	Verified
Email Address Verification Procedures	Not requesting the email trust bit for this root.	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit for this root.	**Verified?**	Not Applicable
Multi-Factor Authentication	NEED: Confirm that multi-factor authentication is required for all accounts capable of directly causing certificate issuance. See # 6 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices	**Verified?**	Need Response From CA
Network Security	NEED: Confirm that you have performed the actions listed in #7 of https://wiki.mozilla.org	**Verified?**	Need Response From CA

/CA:Information_checklist#Verification_Policies_and_Practices

Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs	http://www.visa.com/pki/RootCerts.html	**Verified?**	Verified