



- [Close Window](#)
- [Print This Page](#)
- [Expand All](#) | [Collapse All](#)

R00000066

▼ Information

Case No	00000050	Owner	Kathleen Wilson (Admin)
Root Case No	R00000066	Request Status	Need Information from CA
Root Certificate Name	Visa Information Delivery Root CA		
All Fields Verified?	No		

▼ Fill this section when changing a currently included Root Certificate

Included CA Owner Name	Included Certificate
------------------------	----------------------

▼ Additional Root Case Information

Subject	Include Visa Information Delivery Root CA	Date/Time Opened	11/12/2014 6:29 PM
		Date/Time Closed	

▼ Technical Information about Root Certificate

O From Issuer Field	VISA	O From Issuer Field (Verified?)	Verified
OU From Issuer Field	Visa International Service Association	OU from Issuer Field (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.	Certificate Summary (Verified?)	Verified
Root Certificate Download URL	http://enroll.visaca.com/VisalInfoDeliveryRootCA.crt	Root Certificate Download URL (Verified?)	Verified
SHA-1 Fingerprint	5A:4D:0E:8B:5F:DC:FD:F6:4E:72:99:A3:6C:06:0D:B2:22:CA:78:E4	SHA-1 Fingerprint (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	SHA-256 Fingerprint (Verified?)	Verified
Valid From	6/27/2005	Valid From (Verified?)	Verified
Valid To	6/29/2025	Valid To (Verified?)	Verified
Certificate Version		Certificate Version (Verified?)	Verified
Certificate Signature Algorithm	SHA-1	Cert Signature Algorithm (Verified?)	Verified
Signing Key Parameters	2048	Signing Key Parameters (Verified?)	Verified
Test Website URL (SSL) or Example Cert	https://enroll.visaca.com/	TestWebsiteURL(SSL)orExCert (Verified?)	Verified
CRL URL(s)	http://www.visa.com/pki/revocationlist.html http://Enroll.visaca.com/VICA3.crl http://Enroll.visaca.com/VisalInfoDeliveryRootCA.crl	CRL URL (Verified?)	Verified
OCSP URL(s)	http://ocsp.visa.com/ocsp	OCSP URL (Verified?)	Verified
Trust Bits	Websites	Trust Bits (Verified?)	Verified
SSL Validation Type	OV	SSL Validation Type (Verified?)	Verified
EV Policy OID(s)	Not EV	EV Policy OID(s) (Verified?)	Not Applicable

Root Stores Included In	Microsoft	Root Stores Included In (Verified?)	Verified
Mozilla Applied Constraints	None	Mozilla Applied Constraints (Verified?)	Verified

▼ Test Results (When Requesting the Websites Trust Bit)


Revocation Tested	https://certificate.revocationcheck.com/enroll.visaca.com No OCSP error	Revocation Tested (Verified?)	Verified
CA/Browser Forum Lint Test	This error appears to be a problem in the way we are using the test -- the error is intended for subscriber certs, not root certs Run x509lint: ERROR: Subject with organizationName but without stateOrProvince or localityName	CA/Browser Forum Lint Test (Verified?)	Verified
Test Website Lint Test	Error Unallowed key usage for RSA public key	Test Website Lint Test (Verified?)	Need Response From CA
EV Tested	No EV	EV Tested (Verified?)	Not Applicable

▼ CA Hierarchy Information

CA Hierarchy	CA Hierarchy Diagram in Figure 1-1 of the CP. This root has four internally-operated subordinate Issuing CAs that only issue end-entity certificates: * VI CA1 * VI CA2 * Visa Information Delivery External CA * Visa Information Delivery Internal CA	CA Hierarchy (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.	Externally Operated SubCAs (Verified?)	Verified
Cross Signing	None. CP section 1.1: Cross-certification between external CAs and CAs is not supported. The Visa PKI hierarchy is a closed PKI.	Cross Signing (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.	Tech Cons on 3rd party Iss (Verified?)	Verified

▼ Verification Policies and Practices

Policy Documentation	Documents are in English. The CP refers to this root as "Visa InfoDelivery Root"	Policy Documentation (Verified?)	Verified
CA Document Repository	http://www.visa.com/pki	CA Document Repository (Verified?)	Verified
CP Doc Language	English		
CP	http://www.visa.com/pki/pdf/VisaPublicKeyInfrastructureCertificatePolicy.pdf	CP (Verified?)	Verified
CPS Doc Language	English		
CPS	http://www.visa.com/pki/pdf/VisaPublicKeyInfrastructureCertificatePolicyStatement.pdf	CPS (Verified?)	Verified
Other Relevant Documents		Other Relevant Documents (Verified?)	Not Applicable
Auditor Name	KMPG	Auditor Name (Verified?)	Verified
Auditor Website	http://www.kpmg.com/	Auditor Website (Verified?)	Verified
Auditor Qualifications	http://www.webtrust.org/licensed-webtrust-practitions-international/item64419.aspx	Auditor Qualifications (Verified?)	Verified
Standard Audit	https://bugzilla.mozilla.org/attachment.cgi?id=8640125	Standard Audit (Verified?)	Verified
Standard Audit Type	WebTrust	Standard Audit Type (Verified?)	Verified

Standard Audit Statement Date	7/20/2015	Standard Audit Statement Dt (Verified?)	Verified
BR Audit  infoDelivery		BR Audit (Verified?)	Verified
BR Audit Type	WebTrust	BR Audit Type (Verified?)	Verified
BR Audit Statement Date	4/22/2013	BR Audit Statement Date (Verified?)	Verified
EV Audit		EV Audit (Verified?)	Not Applicable
EV Audit Type		EV Audit Type (Verified?)	Not Applicable
EV Audit Statement Date		EV Audit Statement Date (Verified?)	Not Applicable
BR Commitment to Comply	CPS section 1.1 Comment #43: Updates to CP/CPS in progress	BR Commitment to Comply (Verified?)	Verified
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.	SSL Verification Procedures (Verified?)	Verified
EV SSL Verification Procedures	Not requesting EV treatment for this root.	EV SSL Verification Proc (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).	Org Verification Procedure (Verified?)	Verified
Email Address Verification Procedures	Not requesting the email trust bit for this root.	Email Addr Verification Proc (Verified?)	Not Applicable
Code Signing Subscriber Verification Pro	Not requesting the code signing trust bit for this root.	Code Signing Subs Verif Proc (Verified?)	Not Applicable
Multi-Factor Authentication	Comment #43: we have multi-factor authentication is required for all accounts capable of directly causing certificate issuance	Multi-Factor Authentication (Verified?)	Verified

Network Security

Comment #43: Confirmed that Visa has performed the actions listed in #7 of https://wiki.mozilla.org/CA:Information_checklist#Verification_Policies_and_Practices

Network Security (Verified?)

Verified

▼ Software Release Information

NSS Release When First Included

Firefox Release When First Included

▼ Link to Publicly Disclosed and Audited subordinate CA Certificates

Publicly Disclosed & Audited subCAs

 <http://www.visa.com/pki/RootCerts.html>

Publ Discl & Audited subCAs (Verified?)

Verified

▼ Internal Comments

Comments by Mozilla on Root Case


▼ Public Comments

Comments

▼ System Information

Created By

Poonam Bhargava, 11/12/2014 6:29 PM

Last Sync Date/Time 

Last Modified By

Francis Lee, 7/29/2016 2:57 AM

Root Case History

7/29/2016 2:57 AM	
User	Francis Lee
Action	Changed Test Website Lint Test to Error Unallowed key usage for RSA public key.
7/29/2016 2:36 AM	
User	Francis Lee
Action	Changed BR Audit from NEED: BR audit statement for this root and hierarchy. Please see: https://wiki.mozilla.org/CA:BaselineRequirements Comment #43: Planned for 2016 audit to infoDelivery.
7/25/2016 12:26 AM	
User	Aaron Wu
Action	Changed EV Tested.
7/24/2016 11:47 PM	
User	Aaron Wu
Action	Changed CA/Browser Forum Lint Test to This error appears to be a problem in the way we are using the test -- the error is intended for subscriber certs, not root certs Run x509lint: ERROR: Subject with organizationName but without stateOrProvince or localityName.
7/24/2016 8:19 PM	
User	Aaron Wu
Action	Changed Revocation Tested.