Print this page

Mozilla - CA Program

Case Information

Case Number	00000050	**Case Record Type**	CA Owner/Root Inclusion Request
CA Owner/Certificate Name	Visa	**Request Status**	Information Verification In Process

Additional Case Information

Subject	Include Visa Information Delivery Root CA	**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

CA Email Alias 1	pkipolicy@visa.com		
CA Email Alias 2			
Company Website	http://www.visa.com/	**Verified?**	Verified
Organizational Type	Private Corporation	**Verified?**	Verified
Organizational Type (Others)		**Verified?**	Not Applicable
Geographic Focus	USA, 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.	**Verified?**	Verified

Required and Recommended Practices

Recommended Practices	https://wiki.mozilla.org/CA/Required_or_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	1. Publicly Available CP and CPS: CP/CPS section 2.1 1.1 Revision Table, updated annually: CP/CPS dated 1/31/2018. Revision table not found. 1.2 CAA Domains listed in CP/CPS: NEED: list of issuer domain names recognized in CAA not found in CP/CPS. 2. Audit Criteria: CP/CPS section 8 3. Revocation of Compromised Certificates: CP/CPS section 4.9 4. Verifying Domain Name Ownership: CP/CPS section 3.2.2 (NEED more detail) 5. Verifying Email Address Control: N/A 6. DNS names go in SAN: CP/CPS section 9.6.1, CPS table 7-5 7. OCSP: CP/CPS section 4.9 8. Network Security Controls: CP/CPS section 6.7	**Verified?**	Need Response From CA

Forbidden and Potentially Problematic Practices

Potentially Problematic Practices	https://wiki.mozilla.org /CA/Forbidden_or_Problematic_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	1. Long-lived Certificates: CPS section 6.3.2 2. Non-Standard Email Address Prefixes for Domain Ownership Validation: Not found 3. Issuing End Entity Certificates Directly From Roots: No 4. Distributing Generated Private Keys in PKCS#12 Files: No 5. Certificates Referencing Local Names or Private IP Addresses: CP/CPS section 3.2.2, 9.6.1 6. Issuing SSL Certificates for .int Domains: No 7. OCSP Responses Signed by a Certificate Under a Different Root: No 8. Issuance of SHA-1 Certificates: CP/CPS section 7.1.3 9. Delegation of Domain / Email Validation to Third Parties: CP/CPS section 1.1	**Verified?**	Verified

Root Case Record # 1

Root Case Information

Root Certificate Name	Visa Information Delivery Root CA	**Root Case No**	R00000066
Request Status	Information Verification In Process	**Case Number**	00000050

Certificate Data

Certificate Issuer Common Name	Visa Information Delivery Root CA
O From Issuer Field	VISA
OU From Issuer Field	Visa International Service Association
Valid From	2005 Jun 27
Valid To	2025 Jun 29
Certificate Serial Number	5b57d7a84cb0afd9d36f4ba031b4d6e2
Subject	CN=Visa Information Delivery Root CA, OU=Visa International Service Association, O=VISA, C=US
Signature Hash Algorithm	sha1WithRSAEncryption
Public Key Algorithm	RSA 2048 bits
SHA-1 Fingerprint	5A:4D:0E:8B:5F:DC:FD:F6:4E:72:99:A3:6C:06:0D:B2:22:CA:78:E4
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
Certificate ID	93:81:56:E5:4D:AE:B0:8D:BC:82:67:3C:27:55:84:4F:A3:0A:72:D2:45:66:04:61:FB:A7:83:4F:69:DB:4C:20
Certificate Version	3

Technical Information about Root Certificate

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	**Verified?**	Verified

	Server & Client.		
Root Certificate Download URL	http://enroll.visaca.com /VisaInfoDeliveryRootCA.crt	**Verified?**	Verified
CRL URL(s)	http://Enroll.visaca.com /VisaInfoDeliveryRootCA.crl http://Enroll.visaca.com/VICA3.crl	**Verified?**	Verified
OCSP URL(s)	http://ocsp.visa.com/ocsp	**Verified?**	Verified
Mozilla Trust Bits	Websites	**Verified?**	Verified
SSL Validation Type	OV	**Verified?**	Verified
Mozilla EV Policy OID(s)	Not EV	**Verified?**	Not Applicable
Root Stores Included In	Microsoft	**Verified?**	Verified
Mozilla Applied Constraints	None	**Verified?**	Verified

Test Websites or Example Cert

Test Website - Valid	https://enroll.visaca.com/	**Verified?**	Verified
Test Website - Expired	https://infodelcatest.visaca.com:8443/		
Test Website - Revoked	https://infodelcatest.visaca.com:8444/		
Example Cert			
Test Notes			

Test Results (When Requesting the SSL/TLS Trust Bit)

Revocation Tested	NEED to resolve all errors listed in https://certificate.revocationcheck.com /enroll.visaca.com	**Verified?**	Need Response From CA
CA/Browser Forum Lint Test	NEED: Resolve errors in https://crt.sh/?caid=1302& opt=cablint,zlint,x509lint& minNotBefore=2015-01-01	**Verified?**	Need Response From CA
Test Website Lint Test	NEED: In https://crt.sh/?caid=1302& opt=cablint,zlint,x509lint& minNotBefore=2015-01-01 change caid to 12081, 1303, and 7284 These all have errors that need to be resolved. Note that no errors listed for CA IDs: 1524, 12946, and 49673.	**Verified?**	Need Response From CA

EV Tested	No EV	**Verified?**	Not Applicable

CA Hierarchy Information

CA Hierarchy	CA Hierarchy Diagram in Figure 1-1 of the CP/CPS. This root has internally-operated subordinate Issuing CAs that only issue end-entity certificates: * VI CA1 * VI CA2 * Visa Corporate Email Sub CA * Visa Information Delivery External CA * Visa Information Delivery Internal CA * Information Delivery Sub CA	**Verified?**	Verified
Externally Operated SubCAs	None. CP section 1.1: With the exception of the Visa Smart Debit/Credit (VSDC) PKI, CA certificates can only be issued to Visa or Visa Business Groups.	**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.	**Verified?**	Verified
Technical Constraint on 3rd party Issuer	CP section 1.3.1: A CA PKI administrator must be an employee of Visa. CP section 1.3.2: RA staff must be a Visa employee or contractor.	**Verified?**	Verified

Verification Policies and Practices

Policy Documentation	Documents are in English.	**Verified?**	Verified
CA Document Repository	http://enroll.visaca.com/	**Verified?**	Verified
CP Doc Language	English		
CP	https://www.visa.com/pki/pdf/VisaPublicKeyInfrastructureCertificatePolicy.pdf	**Verified?**	Verified
CP Doc Language	English		
CPS	https://www.visa.com/pki/pdf/VisaPublicKeyInfrastructureCertificatePolicyStatement.pdf	**Verified?**	Verified
Other Relevant Documents		**Verified?**	Not Applicable

Auditor	BDO International Limited	**Verified?**	Verified
Auditor Location	United States	**Verified?**	Verified
Standard Audit	https://bug636557.bmoattachments.org/attachment.cgi?id=8972934	**Verified?**	Verified
Standard Audit Type	WebTrust	**Verified?**	Verified
Standard Audit Statement Date	7/26/2017	**Verified?**	Verified
BR Audit	https://bug636557.bmoattachments.org/attachment.cgi?id=8972936	**Verified?**	Verified
BR Audit Type	WebTrust	**Verified?**	Verified
BR Audit Statement Date	7/26/2017	**Verified?**	Verified
EV SSL Audit		**Verified?**	Not Applicable
EV SSL Audit Type		**Verified?**	Not Applicable
EV SSL Audit Statement Date		**Verified?**	Not Applicable
BR Commitment to Comply	CP/CPS section 1.1 Note in CPS section 1.1: ...this CPS document takes precedence over the Baseline Requirements.	**Verified?**	Verified
BR Self Assessment	https://bugzilla.mozilla.org/attachment.cgi?id=8893903	**Verified?**	Verified
SSL Verification Procedures	CP/CPS section 3.2.2 -- not enough information to understand what the Visa CA does to verify domain ownership control. NEED: CP needs to say *how* the domain verification is done. Listing the types of domain verification allowed (per the BRs) does not say how the Visa CA actually does any of them.	**Verified?**	Need Response From CA
EV SSL Verification Procedures	N/A	**Verified?**	Not Applicable
Organization Verification Procedures	CP/CPS sections 3.2.2, 3.2.3, 3.2.5	**Verified?**	Verified
Email Address Verification Procedures	N/A	**Verified?**	Not Applicable
Code Signing Subscriber Verification Pro	N/A	**Verified?**	Not Applicable
Multi-Factor Authentication	CP/CPS section 5.2	**Verified?**	Verified
Network Security	CP/CPS section 6.7	**Verified?**	Verified