**General information about the VISA InfoDelivery Root CA**

1. **Name:**

Visa Information Delivery Root CA

2. **Website URL:**

<http://www.visa.com>

3. **Organizational type:**

The CA is operated by a private corporation (Visa Inc.)

4. **Primary market / customer base:**

Which types of customers does the CA serve:

The inclusion of these certificate authorities will enable Mozilla’s consumers to authenticate to Visa products and services.

Are there particular vertical market segments in which it operates:

Financial services

Does it focus its activities on a particular country or other geographical region:

No, the CA is global.

5. **Impact to Mozilla users:**

Describe the types of Mozilla users who are likely to encounter your root certificate as relying parties while web browsing (HTTPS servers doing SSL), sending/receiving email to their own MTA (SMTPS, IMAPS servers doing SSL), sending/receiving S/MIME email (S/MIME email certs), etc.:

Any Visa issuing bank using any of Visa's secured web based services. **CA Contact Information:**

|  |  |  |
| --- | --- | --- |
| Visa Inc.  P.O. Box 8999  San Francisco, CA 94128-8999 | Michael Stefanich  mstefani@visa.com  (303) 389-7750 | Richard Burgos  rburgos@visa.com  (303) 389-7723 |

**Technical information about the Visa InfoDelivery Root CA certificate**

1. **Certificate Name:**

Visa Information Delivery Root CA

1. **Certificate Issuer Field**

CN = Visa Information Delivery Root CA

OU = Visa International Service Association

O = VISA

C = US

1. **Certificate Summary**

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.

The Visa Information Delivery Root CA which provides Certificate Signing, Off-line CRL Signing, CRL Signing (06) has several subordinate online CAs that issue end entity certificates (SSL client, SSL server, digital signature, VPN/IP Sec, SSL Server & Client).

The Visa Information Delivery Root was created in 2005 and has passed WebTrust Audits conducted by KPMG from 2005 through 2010. The WebTrust report is not publicly accessible but can be provided upon request. Visa’s Certificate Policy is publicly accessible from http://www.visa.com/pki. The Visa Certification Practice Statement is not publicly accessible but can be provided if required.

1. **Root Certificate URL**
   * <http://enroll.visaca.com>
2. **SHA1 fingerprint**

5a 4d 0e 8b 5f dc fd f6 4e 72 99 a3 6c 06 0d b2 22 ca 78 e4

1. **Valid from (YYYY-MM-DD)**

Monday, June 27, 2005 17:42:42 GMT

1. **Valid to (YYYY-MM-DD)**

Sunday, June 29, 2025 17:42:42 GMT

1. **Certificate Version (should be 3)**

V3

1. **Certificate Signature Algorithm**

sha1RSA

1. **Signing key parameters**

2048 bits

1. **Test website URL -- if you are requesting to enable the Websites (SSL/TLS) trust bit**
   * + <http://enroll.visaca.com>
2. **Example certificates**
   * If this root does not issue certificates for SSL, then provide example certificate(s) issued within the hierarchy rooted at this root, including the full certificate chain(s).

Visa will provide end-entity certificates from our issuing Certificate Authorities for the chain validation testing requirement by a separate e-mail.

1. **Certificate Revocation Lists (CRLs)**
   * URL(s) at which the CRL(s) may be obtained -- for end-entity certs and for intermediate CAs.

http://enroll.visaca.com/ , and

http://crl.inov.visa.net/ , as well as

ldap://enroll.visaca.com/ , and

ldap://crl.inov.visa.net/

* + The value that nextUpdate is set to in the CRLs for end-entity certificates.

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.

* + The sections of your CP/CPS documentation that state the requirements about frequency of updating CRL.

Certification Practice Statement, Chapter 4, Certificate Revocation List (CRL) Issuance Frequency.

* + Note the [CA/Browser Forum's EV guidelines:](http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf) CRLs MUST be updated and reissued at least every seven days, and the nextUpdate field value SHALL NOT be more ten days
  + You must test your CRLs by importing them into the Firefox browser.
    - [Error Codes:](http://www.mozilla.org/projects/security/pki/nss/ref/ssl/sslerr.html)
      * ffffe095, is equivalent to -8043, SEC\_ERROR\_CRL\_UNKNOWN\_CRITICAL\_EXTENSION Resolution: See [Potentially Problematic Practice CRL with Critical CIDP Extension](https://wiki.mozilla.org/CA:Problematic_Practices#CRL_with_critical_CIDP_Extension)
      * 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.

1. **OCSP (OCSP is required for EV enablement)**

Not applicable. Visa is currently not planning to issue EV certificates from the Visa InfoDelivery Root CA.

1. **Requested Trust Bits**
   * State which of the three trust bits you are requesting to be enabled for this root. One or more of:
     + Websites (SSL/TLS)
     + Email (S/MIME)
     + Code Signing

The Visa Information Delivery Root CA which provides Certificate Signing, Off-line CRL Signing, CRL Signing (06) has several subordinate online CAs that issue end entity certificates (SSL client, SSL server, digital signature, VPN/IP Sec, SSL Server & Client).

* + Mozilla’s standpoint is that we should operate the root program in terms of minimizing risk. One way that we can minimize risk is by not enabling more trust bits than CAs absolutely require.

1. **SSL Validation Type**
   * Indicate the levels of SSL validation that are used for certificates within this root's hierarchy. One or more of:
     + OV -- In addition to verifying the domain ownership, you also validate the organization to be listed in the O field - making sure public record and government resources can verify the address, existence, and good legal standing of the organization itself. Verifying that the whois listed address matches the verified address, and any other additional checks that a given CA lists in its CPS.

1. **If EV certificates are issued within the hierarchy rooted at this root, the EV policy OID(s) associated with those EV certificates.**

N/A.

**CA hierarchy information for the Visa InfoDelivery Root CA certificate**

1. CA Hierarchy
   * A description of the PKI hierarchy rooted at or otherwise associated with this root CA certificate.
     + List and/or describe all of the subordinate CAs that are signed by this root.
     + Identify which of the subordinate CAs are internally-operated; e.g. list the subordinate CAs that operated by the CA organization associated with the root CA. For example, this might include subordinate CAs created to issue different classes or types of end entity certificates to the general public: Class 1 vs. class 2 certificates, qualified vs. non-qualified certificates, EV certificates vs. non-EV certificates, SSL certificates vs. email certificates, and so on.

It might also include subordinate CAs operated for the benefit of specific third parties. In this case note that we do *not* require that the CA submit a complete customer list; rather we are interested in the general type and nature of the third-party arrangements.

The Visa Information Delivery Root CA has two subordinate Issuing CAs:

(1) VICA1 – Visa Inc. Certificate Authority for Internet use – VI CA1

(2) VICA2 – Visa Inc. Certificate Authority for Intranet use – VI CA2

These two CA’s are internally operated Issuing CAs and issue only end-entity certificates.

1. Sub CAs Operated by 3rd Parties
   * If this root has any subordinate CAs that are operated by external third parties, then provide the information listed in the [Subordinate CA Checklist](https://wiki.mozilla.org/CA:SubordinateCA_checklist)
   * If the CA functions as a super CA such their CA policies and auditing don't apply to the subordinate CAs, then those CAs must apply for inclusion themselves as separate trust anchors.

N/A. Visa does not permit sub CAs operated by 3rd parties.

1. Cross-Signing
   * List all other roots for which this root CA has issued cross-signing certificates.
   * List all other root CAs that have issued cross-signing certificates for this root CA.
   * If any such roots exist, it is important to note whether the roots in question are already included in the Mozilla root store or not.

N/A. Visa does not permit cross signing Certificate Authorities.