060308-Info CP01

Visa Inc

Visa Inc.
Public Key Infrastructure (X.509)
Certificate Policy

Information Delivery PKI

2.23.131.2.1

February 27, 2009
Version 2.0

Visa Inc. PKI Certificate Policy
Information Delivery PKI
1.1.1.4

Revision History

Version	Date	Author's initials	Description of changes
0.1	2005-09-08	AT (Visa)	Initial Working Draft
1.0	2006-01-27	AT (Visa)	Revised based upon feedback from Inovant
1.1.1	2006-08-07	GC/RL (RSA)	Conversion to RFC 3647
1.1.2	2006-12-15	AT	Update section 7.1.1
1.1.3	2008-04-11	R Sweeney	Visa Inc, Cryptographic Review Board, Client
2.0	2009-02-27	M. Alvarado	Changed PKI Policy Committee to Cryptographic Review Board

Table of Contents

CERTIFICATE POLICY SUMMARY

This document contains policies pertaining to the issuance and use of Visa X.509 digital certificates. The intended audience for this document includes Visa Regions, Visa subsidiaries, Clients, and their agents who use these certificates in conjunction with Visa products and services. This certificate policy assumes that the reader has a basic knowledge of digital signatures, certificates, and Public Key Infrastructures (PKI).

Overview

Visa Inc has implemented an X.509 Public Key Infrastructure (PKI) for issuing and distributing digital certificates in support of strong authentication for Visa products and services. This infrastructure is known as the **Visa Inc Information Delivery PKI** or **InfoDelivery PKI** and consists of a hierarchy of entities called Certification Authorities (CAs). A CA is a trusted third party that issues digital certificates to Subscribers (end entities or other CAs) within the hierarchy. End entity Subscribers are individuals or organizations that obtain certificates for use with Visa products and services.

At the top of the Visa InfoDelivery PKI hierarchy is the Visa Inc. CA (**Visa Inc CA**), which includes the **Visa Root CA** and the **Visa Brand CAs**. Visa Brand CAs are directly subordinate to the Visa Root CA. Visa Region and Client CAs may also participate in the Visa PKI and are subordinate to the Visa Brand CAs. These CAs are referred to as "**Participating CAs**". Figure 1 illustrates the conceptual Visa InfoDelivery PKI hierarchy and demonstrates the Visa Inc CA component, as well as where the Visa Region and Client CAs may participate in the hierarchy.

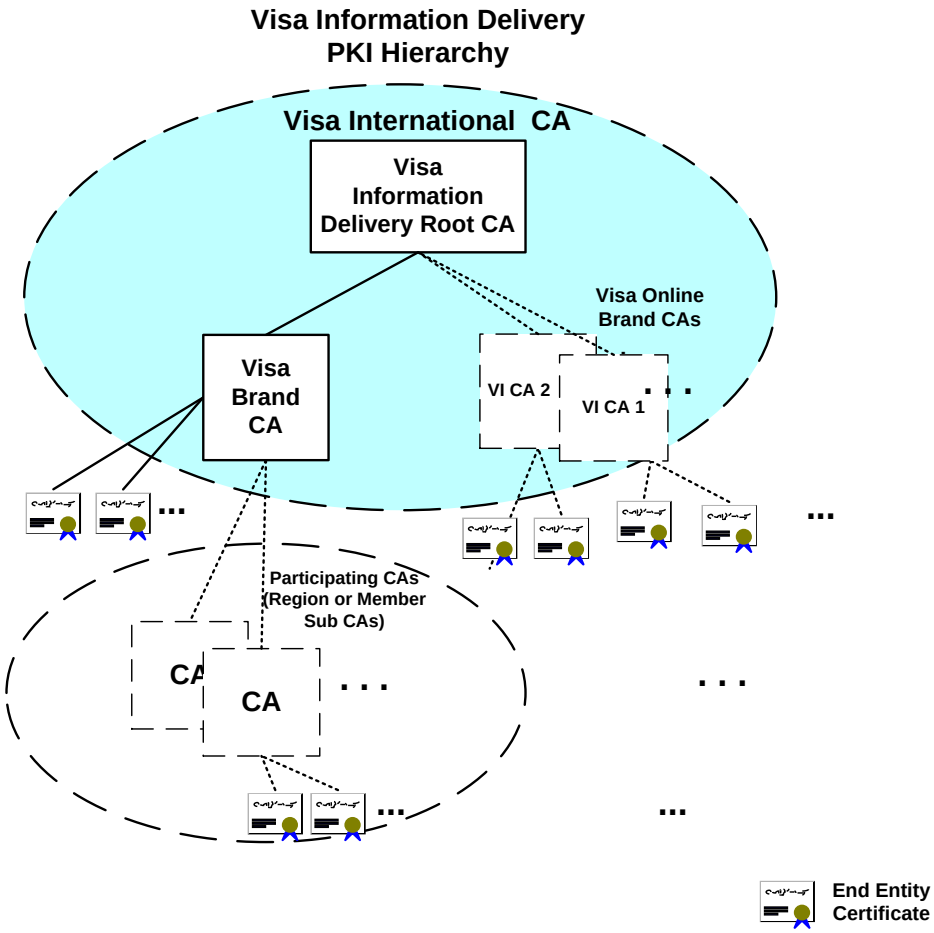

Figure 1 - Visa Information Delivery PKI Hierarchy

In this hierarchal model, all entities trust the Visa Root CA (top of the hierarchy). With the exception of the Visa Root CA, all CAs are subordinate to one superior CA, which signs the public key (creating a CA certificate) corresponding to the private key of the subordinate CA. The Visa Root CA will issue CA certificates to Visa Brand CAs. Visa Brand CAs may issue certificates to subordinate CAs or to end entity Subscribers. The third-tier CAs are optional and are referred to as "Participating CAs". Participating CAs and online Visa Brand CAs are not permitted to issue certificates to subordinate CAs and must only issue to end entity Subscribers. The issuing of a certificate to a subordinate CA or end entity Subscriber creates a trust relationship between the issuing CA and that subordinate entity. A "certificate chain" is created from the Visa Root CA to the lowest entity in the hierarchy, since all certificates are signed by a superior CA, which eventually terminates with the Visa Root CA. This is referred to as a hierarchal trust model. Each trust relationship is represented as a line in figure 1, and consists of a single certificate.

This document is the Certificate Policy (CP) for the Visa InfoDelivery PKI. The CP contains policies pertaining to the business, and technical requirements for approving, issuing, managing, revoking and renewing digital certificates as well as key pair and certificate life cycle management. These certificates are used to authenticate the participants in a transaction as well as to protect the confidentiality and integrity of the transaction itself as it is being transmitted over a network. The Visa Inc. Cryptographic Review Board is the managing entity of policies for all of the Visa X.509 PKI hierarchies. The target audience for this document is Visa entities; that is Visa

Regions, Visa subsidiaries, Visa Clients and their agents who use certificates associated with the Visa InfoDelivery PKI in conjunction with Visa products and services.

The CP is the first in a set of documents relevant to the Visa InfoDelivery PKI. As can be seen in figure 2, the CP (red spanning arrow) encompasses policy for the entire PKI. Other documents, such as a Certificate Practice Statement (CPS), are specific to the functioning of a particular CA. The CPS (blue spanning arrows) explains the practice a particular CA employs in providing certification services, in order to meet the requirements of the CP. Other ancillary documents, such as general security policies, operation procedures, key ceremony guides, disaster recovery plans, etc, may also supplement the CP and CPS.

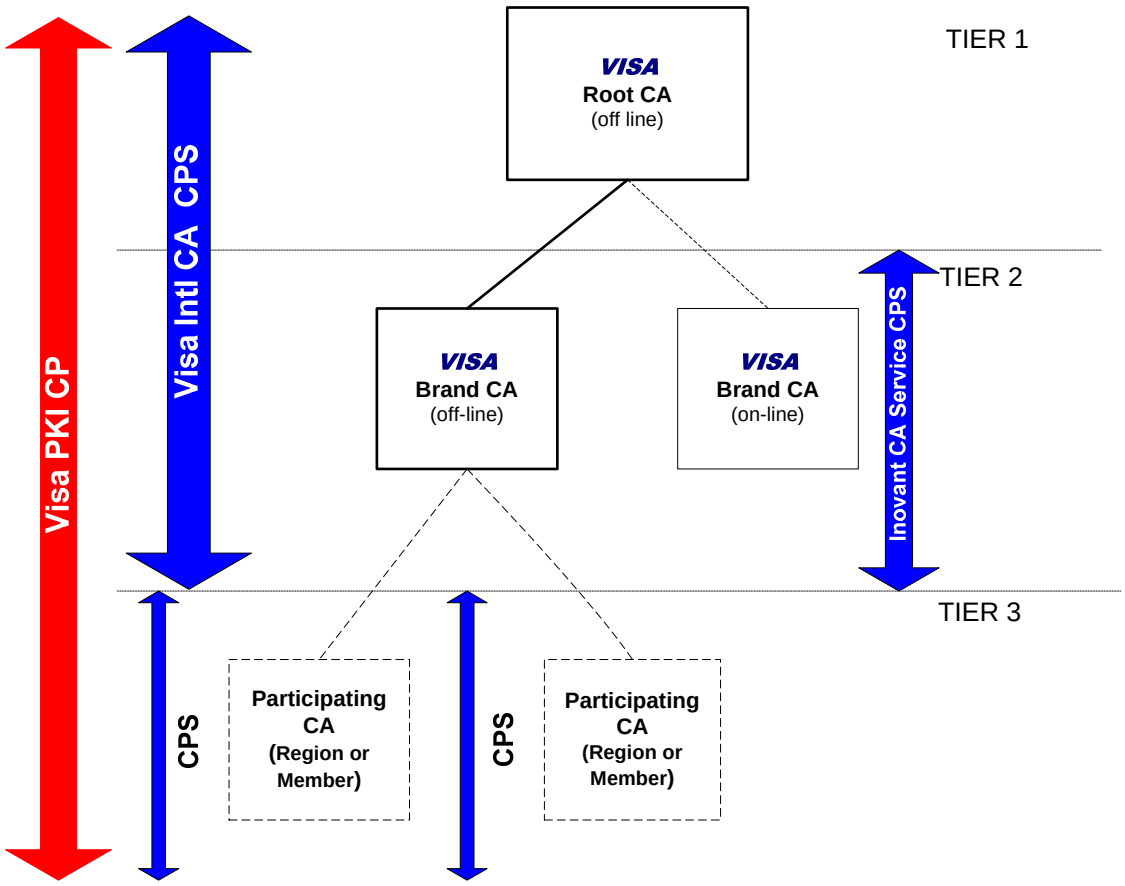

Figure 2 - Visa Document Structure

The Visa InfoDelivery PKI CP generally conforms to the IETF PKIX Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework (also known as RFC 3647). This document is divided into nine sections:

Section 1 - provides an overview of the policy and set of provisions, as well as the types of entities and the appropriate applications for certificates.

Section 2 - contains any applicable provisions regarding identification of the entity or entities that operate repositories; responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status; frequency of publication; and access control on published information.

Section 3 - covers the identification and authentication requirements for certificate related activity.

Section 4 - deals with certificate life-cycle management and operational requirements including application for a certificate, revocation, suspension, audit, archival and compromise.

Section 5 - covers facility, management and operational controls (physical and procedural security requirements).

Section 6 - provides the technical controls with regard to cryptographic key requirements.

Section 7 - defines requirements for certificate, Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP) formats. This includes information on profiles, versions, and extensions used.

Section 8 – addresses topics covered and methodology used for assessments/audits; frequency of compliance audits or assessments; identity and/or qualifications of the personnel performing the audit or assessment; actions taken as a result of deficiencies found during the assessment; and who is entitled to see results of an assessment.

Section 9 - covers general business and legal matters: the business issues of fees, liabilities, obligations, legal requirements, governing laws, processes, and confidentiality.

POLICY SPECIFICATION

1 INTRODUCTION

1.1 Overview

The Visa InfoDelivery PKI CP provides the framework and context within which certificates are requested, created, issued, renewed, managed, and/or used by all participants of this Visa PKI, in particular certificates issued by the Visa International CA (Visa Root CA and Visa Brand CAs), or other participating CAs subordinate to a Visa Brand CA (see figure 1). Specifically, this CP describes the business and technical requirements for the Visa Inc. CA and participating CAs in conjunction with their CPS, Visa Inc. By-Laws, Operating Regulations and policies.

Visa InfoDelivery PKI CAs (CAs within the Visa InfoDelivery PKI hierarchy) issue certificates for use in conjunction with various Visa products and services that require security services. These certificates are used to authenticate the participating entities in an online transaction, to provide session confidentiality for the data being communicated, and to provide message integrity for the transaction. Visa certificates (i.e., those certificates issued within the Visa InfoDelivery PKI hierarchal trust model as shown in figure 1) can only be used in conjunction with Visa products and services unless the Visa Inc. Cryptographic Review Board grants specific prior approval.

The Visa InfoDelivery PKI hierarchy, like Visa itself, is a closed environment. Certificates can only be issued to entities that have a contractual agreement with Visa, or Visa Regions and/or Clients, and are bound to comply with Visa Inc By-laws, Operating Regulations and policies. End entity certificates (i.e., those which can only be used for authentication or to provide data confidentiality or message integrity) can be issued to Visa Regions, Visa Clients and their agents, as well as employees, merchants, and cardholders who have a valid business relationship with Visa and are contractually bound to comply with Visa Inc By-laws, Operating Regulations and policies. CA certificates (i.e. those which can be used to sign other certificates or certificate revocation lists) can only be issued to Visa Inc, Visa Regions and/or Visa Clients. Reliance upon certificates issued within any Visa PKI is limited to entities that have agreed to comply with Visa Inc By-laws, Operating Regulations and policies. No other person or entity may rely upon a certificate issued within any Visa PKI for any purpose.

The types of certificates issued will vary depending upon the product and service being delivered; however, the request process itself is independent of product. How the certificate requests are received, processed and returned to the Subscribers is the same for all Visa products but may vary from an automation perspective based on a particular CA system configuration. The CA's CPS will describe these processes in more detail. The types of certificates requested and the entities to which they are issued are specific to the Visa product and / or service requirements and will also be described in the issuing CA's CPS.

Sections that have a heading *SIGNATURE* contain information pertaining only to a digital signing policy. A digital signing policy is designed to define the rules for signing certificates, documents and objects with a private key. Sections that have a heading *CONFIDENTIAL* pertain only to a confidentiality policy. Confidentiality policy describes the use of a private encryption key for protecting information and documents. All other sections apply to both *SIGNATURE* and *CONFIDENTIAL*.

1.2 Document name and identification

This CP is titled Visa Inc InfoDelivery Public Key Infrastructure Certificate Policy or "**Visa InfoDelivery PKI CP**".

The object identifier (OID) used for certificates issued under this CP is: **2.23.131.2.1**

1.3 PKI participants

The communities governed by this CP are the Visa InfoDelivery Root CA and Visa Brand CAs (direct subordinate CAs), participating CAs (subordinate to a Visa Brand CA), and all Subscribers issued certificates by a CA in this Visa PKI. Under this CP, the Visa InfoDelivery Root CA will not issue end entity certificates. This Root CA will only issue subordinate CA certificates to Visa Brand CAs. An offline Visa Brand CA may issue to subordinate CAs (participating CAs) and end entities (Visa Regions, Clients, and their agents) that have contractual agreements with Visa or its Clients and are bound to comply with Visa Inc By-Laws, Operating Regulations and policies. Visa online Brand CA may issue certificates to end entities (Visa Clients and their agents) that have contractual agreements with Visa or its Clients and are bound to comply with Visa Inc By-Laws, Operating Regulations and policies.

A participating CA may also issue, recognize and support additional Certificate Policies, as long as these are not in conflict with this Visa InfoDelivery PKI CP.

1.3.1 Certification Authorities (CAs)

Each Visa PKI consists of a hierarchy of CAs, which sign certificates that bind Subscribers (e.g. Visa Regions, Clients and their agents) to their private keys.

CAs, operating within and under a Visa PKI, are responsible for:

SIGNATURE

- Creating and signing of certificates binding Subscribers and as required subordinate CAs to their signature verification keys;
- Publishing certificate status through certificate revocation lists (CRLs) or other commonly implemented methods such as online certificate status protocol (OCSP), if supported by Relying Party applications; and
- Requiring adherence to this certificate policy.

CONFIDENTIAL

- Creating, storing and recovering end entity confidential key pairs if required;
- Promulgating certificate status through CRLs or other commonly implemented methods such as OCSP, if supported by Relying Party applications; and
- Creating and signing of certificates binding Subscribers to their public encryption key.
- Requiring adherence to this certificate policy.

1.3.2 Registration Authorities (RAs)

An RA is an entity approved by a CA to assist in the verification of certificate request content (applicant information) on behalf of a CA. The primary responsibility of the RA is to verify that the party submitting the certificate request is who it claims to be and is authorized to submit the request on behalf of the certificate request originator, has a valid business relationship with Visa consistent with the certificate being requested, and that the certificate request has been transferred from the originator to the RA or RA system (i.e., enrollment server) in a secure manner. The RA is also tasked to verify certificate revocation requests in a similar manner. An RA operating under this CP may also be responsible for other duties delegated to it by the issuing CA.

An RA may perform duties on behalf of more than one CA, providing that in doing so it satisfies all requirements of this CP and it is not otherwise contractually prohibited from doing so.

RAs shall be personnel employed by Visa Inc Visa Regions, Visa subsidiaries or Visa Clients, and must be contractually bound to comply with the Visa Inc By-Laws, Operating Regulations and policies.

1.3.3 Subscribers

A Subscriber is an entity; that is, single person, device or application that is a holder of a private key corresponding to a public key, and has been issued a certificate. In the case of a device, a person authorized by the organization owning the device may be referred to as the Subscriber.

There are two categories of Subscribers: end entities and certification authorities. End entity Subscribers have certificates that can only be used for authentication, confidentiality or message integrity. End entity Subscribers include:

- Individuals (i.e., employees of the Visa Brand, Regions, Clients or their agents)
- Organizations (i.e., merchants, Visa Regions and Clients or their agents)
- Devices or applications (e.g., servers, client software) to be used by the Visa Brand, Region, Clients or its agent in conjunction with the delivery of a Visa product or service. In each case the certificate binds a key pair to a single functional entity.

Certification Authority Subscribers have certificates that allow them to sign other certificates and/or certificate revocation lists. Certification Authority Subscribers may also have certificates that can be used for authentication, confidentiality or message integrity. Certification Authority Subscribers include:

- Visa InfoDelivery Root CA and offline Brand CAs which will issue certificates to subordinate Certification Authorities in the Visa InfoDelivery PKI
- Participating CAs (Region or Clients CAs subordinate to Visa offline Brand CAs) and Visa online Brand CAs that will only issue end entity certificates.

A CA may administer any number of Subscribers. Responsibility and accountability for each certificate shall be attributable to an identified entity.

Subscriber eligibility for a certificate is at the sole discretion of the issuing CA, and applicable RA, as long as it is consistent with Visa's overall policies regarding participation in the Visa PKI hierarchy. Subscribers shall have a valid business relationship with Visa and must be contractually bound to comply with the Visa Inc By-Laws, Operating Regulations and policies.

1.3.4 Relying Parties

Relying Parties are persons or entities that act in reliance upon a certificate or digital signature (including by means of devices under their control). Relying Parties within any Visa PKI must have a valid business relationship with Visa and be contractually bound to comply with the Visa Inc By-Laws, Operating Regulations and policies.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

This CP is applicable for the Visa InfoDelivery CA (Visa InfoDelivery Root and Visa Brand CAs) and participating CAs that are integral part of the Visa InfoDelivery PKI. The policies described in this CP apply to the issuance, utilization and revocation of certificates within the Visa InfoDelivery PKI.

1.4.1 Appropriate certificate uses

For Visa InfoDelivery CA and participating CAs, this CP is suitable for:

SIGNATURE

Protecting the integrity and authenticity of business transactions.

CONFIDENTIAL

Providing confidential transfer of information.

1.4.2 Prohibited certificate uses

Certificates issued under this CP by a CA within Visa InfoDelivery PKI are prohibited under any other use not specified in Section 1.4.1.

1.5 Policy administration

Visa Inc. Cryptographic Review Board is the overall administrative authority of this CP.

1.5.1 Organization administering the document

Visa Inc. Cryptographic Review Board is the responsible authority for reviewing and approving changes to the Visa InfoDelivery PKI CP. Written and signed comments on proposed changes shall be directed to the Visa Inc CA contact as described in Section 1.5.2. Decisions with respect to the proposed changes are at the sole discretion of the Visa.Inc. Cryptographic Review Board

1.5.2 Contact person

The following is the primary contact for the Visa Inc PKI Support.

Visa Inc.
Global Information Security – Security EngineeringTechnology Management
8910 South Ridgeline Boulevard 900 Metro Center
Highlands Ranch, CO 80129
(303) 389 7750
PKIPolicy@visa.com

1.5.3 Person determining CPS suitability for the policy

Visa Inc. Cryptographic Review Board is the administrative entity for determining CPS suitability to this CP.

1.5.4 CPS approval procedures

Visa Regions or Clients wishing to become a participating CA within the Visa InfoDelivery PKI hierarchy shall sign an agreement with the Visa Inc. Cryptographic Review Board (i.e., a Subscriber agreement) and submit a proposed CPS in accordance with this CP describing the functioning of the CA. The Visa Inc. Cryptographic Review Board shall approve or reject the proposed CPS within its sole discretion and may require an onsite audit.

The Visa Inc CA will review any modifications, additions or deletions from a Visa Inc CA CPS or Participating CA CPS, and determine if modifications, additions or deletions are acceptable and do not jeopardize operations or the security of the CA environment.

Where a CA's CPS contains confidential information regarding the security controls of the CA, the CPS need not be made publicly available in whole or in part.

1.6 Definitions and acronyms

A list of definitions and acronyms can be found at the end of this document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

A CA shall have at least one certificate repository (e.g. CA database, LDAP directory) and one certificate status repository associated with the CA. A repository may or may not be on the same hosting system as the CA, and either certificates or CRLs may be published to a remote repository such as a standards-based LDAP directory or an OCSP responder (for certificate status information). CRLs may be published to a Visa web site to facilitate accessibility. Where the certificate repository is operated in a different computing environment other than the CA, the repository shall remain under control of the Visa InfoDelivery PKI environment.

The CA:

- Shall make available, to Relying Parties, certificate revocation information (e.g., CRLs) published by the CA in accordance with the requirements of Section 4.9 and 4.10; and
- Shall make available a copy of the Visa Inc PKI Disclosure Statement and/or the CA's CPS for Subscriber and Relying Party review. The Visa PKI Disclosure Statement is available at www.visa.com/pki.

2.2 Publication of certification information

Subscribers shall be notified that a CA may publish information submitted by them to publicly accessible directories in association with certificate status information. The publication of this information will be within the limits of section 9.3 and 9.4.

CRL publication shall be in accordance with Section 4. A CA will publish certificate status information in frequent intervals as indicated in its CPS.

Visa InfoDelivery CA retains an online repository of documents where it makes certain disclosure about its practices, procedures and the content of certain of its policies including its CPS and this CP. Visa PKI reserves the right to make available and publish information on its policies by any means it sees fit. Due to their sensitivity, Visa Inc.l may refrain from making publicly available certain subcomponents and elements of such documents including, but not limited to, certain security controls and procedures related with the CA functioning.

2.3 Time or frequency of publication

Certificates information shall be distributed and/or published promptly upon issuance. Maximum time limits and frequency will be described in the respective Visa InfoDelivery CA or Participating CA CPS.

Updates to this CP are published in accordance with section 9.12. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary.

2.4 Access controls on repositories

A CA keeps access to its public repository available to Relying Parties with the purpose of validating issued certificate. A CA may limit or restrict access to its services such as the publication of status information on third party databases, and private directories.

Access controls may be instituted at the discretion of a CA with respect to certificate status. Certificates shall be distributed and/or published promptly upon issuance. A CA shall use commercially reasonable efforts to provide Relying Parties unrestricted access either directly or by agreement, to certificate status information (e.g., CRLs). Certificate status publication shall be in accordance with Section 4. An issuing CA shall provide a full text version of this CP and its CPS when necessary for the purposes of audit, accreditation or as required by law.

3 IDENTIFICATION AND AUTHENTICATION

A Subscriber is described as a person, system, device, or organization to which Visa InfoDelivery PKI end entity or CA certificates can be issued. Visa InfoDelivery PKI Subscribers can be:

- Individuals associated directly with or through the agents of the Visa Brand, a Region or a Client; (e.g., cardholders, merchants and employees)
- Organizations (e.g., Visa Regions and Clients or their agents, merchants)
- Devices or applications (e.g., servers, client software) to be used by the Visa Brand, a Region, a Client or agents for any of the aforementioned in conjunction with the delivery of a Visa product or service. In each case the subscriber must be a single functional entity—key pairs and certificates shall not be shared among multiple functional entities.
- A subordinate CA; in the case of the Visa InfoDelivery Root CA, the Subscriber is a subordinate Visa Brand CA. A participating CA is a Subscriber to a Visa Brand CA.
- Visa personnel issued certificates for the purpose of administering a CA.

In all cases, the certificate request itself must be submitted by an individual either on their own behalf or on the behalf of the Visa organization, device or application that will use the certificate.

This section describes the requirements for authentication of the certificate requester. In those cases where the certificate requester will not be the Subscriber, it also describes the requirements for establishing that the certificate requester is authorized to submit the request on-behalf of the eventual Subscriber.

3.1 Naming

3.1.1 Types of names

Each certificate shall have a clearly distinguishable and unique name for the Subscriber in the certificate subject name field. This name shall be in form of an X.501 Distinguished Name (DN) in accordance with the IETF PKIX standard, supporting a hierarchal naming structure. Each Subscriber may also use an alternative name via the Subject Alternative Name extension attributes, which also shall be in accordance with the IETF PKIX standard. The DN shall not be blank and shall be in the form acceptable to the X.501 standard (printableString or UTF8String).

Examples of subject name fields or attributes (DN components also referred to as Relative Distinguished Name (RDN)) are:

- Common Name (user or device name)
- User ID
- Organizational Unit
- Organization
- Locality
- State or Province
- Country

3.1.2 Need for names to be meaningful

In all cases, names of subjects shall be meaningful. Generally, the name of record (i.e., authenticated name) by which a Subscriber is commonly known to Visa Inc or a Visa Region or Client shall be used. The Visa InfoDelivery PKI does not allow the use of pseudonyms in Subscriber common names. For specific CAs (Visa Brand CAs or participating CAs), within this Visa PKI, the respective CPS may specify additional structure to the naming convention such as inclusion of the Visa Region or Client name. In exceptional cases where the identity of the Subscriber is protected, the name could be a combination of alphanumeric characters.

3.1.3 Anonymity or pseudonymity of subscribers

In exceptional cases where the identity of the Subscriber is protected; the name could be a combination of alphanumeric characters.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The subject name or DN shall be unique for all Subscribers of each CA. If applicable, for each Subscriber where the naming components are similar, additional numbers or letters may be appended to provide uniqueness (in most cases this would be done in the Common Name (CN) attribute) or via the Unique ID (UID) attribute.

3.1.6 Recognition, authentication and roles of trademarks

The priority to use specific entity names will be given to the registered trademark holders.

The use of a Domain Name is restricted to the authenticated legal owner of that Domain Name.

The use of an email address is restricted to the authenticated legal owner of that email address.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The method to prove possession of a private key shall be PKCS #10, or another cryptographically equivalent request (digitally signed request with private key).

3.2.2 Authentication of Visa Organizational Identity

An application for a Visa organizational entity (i.e. Visa Client, Visa Region) to become a Subscriber shall be made by a person authorized to act on behalf of the organization. The application must include details about the Visa organization, in a form, as requested by the Visa Inc Cryptographic Review Board. The details must be provided in a secure manner (i.e., S/MIME or equivalent protected file), or via a separate written document (appropriately marked confidential).

Identification and authentication of an applicant shall follow Section 3.2.2 as if that individual was applying for the certificate on their own behalf.

An issuing CA or an RA on behalf of the issuing CA shall verify the identity of the individual making the application, the validity of that Visa organization's business relationship with Visa Inc.l, and their authority to receive the certificate(s) for that Visa organization.

The RA and CA shall keep a record of the type and details of the identification used for the authentication of the Visa organization for at least the life of the issued certificate.

3.2.3 Authentication of individual identity

An application to become a Subscriber may be requested by an authorized individual of a Visa Region, Visa Member Client or their agents, as well as employees, merchants or cardholders. Individuals shall only be end entity Subscribers; that is they may only 'own' certificates that can be used for authentication, data confidentiality or message integrity. A Subscriber shall have a contractual agreement with Visa Inc., a Visa Region or Client, and is bound to comply with Visa Inc and Regional Operating Regulations and Visa Inc policies. The types of certificates issued by the CA may vary depending upon the Visa product and/or service requirement; however, the request process itself is independent of product and/or service requirement. The process of how

the certificate requests are received, processed and returned to the Subscriber is the same for all certificates

The Subscriber is responsible for:

1. Generating a request that meets this Visa PKI's requirements for a certificate request.
2. Delivering the request to the RA or RA system in a secure manner (e.g., S/MIME or equivalent protected file if offline or SSL/TLS session to enrollment server if online).
3. Demonstrating that this request is authentic.

The RA has the responsibility, on behalf of the Visa InfoDelivery CAs and participating CAs, for:

4. 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 (e.g., security audit).
5. Authenticating the entity submitting the request in accordance with the Identification and Authentication procedures specified for the type of certificate and/or the Visa product or service with which the certificate is intended to be used.
6. Verifying that the certificate request has been transferred from the Subscriber to the RA or RA system (i.e., enrollment server) in a secure manner (e.g., S/MIME or equivalent protected file for offline CAs and SSL/TLS session to enrollment server if online). The security requirements regarding how that request is to be securely transmitted from the Subscriber to the CA, are Visa product and service dependent and will be described in the issuing CA's CPS.
7. If the CA is offline, submitting the certificate request, along with the appropriate documentation to the Visa InfoDelivery CA or participating CA in a secure manner (e.g., S/MIME or equivalent protected file).

The CA and RA shall keep a record of the Certificate Services Work Order (or other appropriate documentation as specified for the Visa product and/or service and type of certificate to be issued) and details of identification used for the authentication of the individual for at least the life of the issued certificate.

3.2.4 Non-verified subscriber information

A CA will identify in its CPS the submitted Subscriber information that is not verified as part of a certificate request.

3.2.5 Validation of authority

An application for a certificate, to be used by a Visa product or service component (processor, server, device, application, etc.), shall be made by an individual that is accountable, authorized and responsible for the component participating in the Visa product or service. The authorization will be required to be an official appointment of such (e.g., company/organization letter signed by an organizational authority).

3.2.6 Criteria for interoperation

The Visa InfoDelivery PKI hierarchy is a closed PKI. Cross Certification between external CAs and a Visa CA and/or participating CAs will **not** be supported.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Prior to the expiry of a certificate associated with a particular public/private key pair, a new certificate request using a new key pair shall be submitted by an authorized individual of the Visa Region, Visa Client or their agents representing the particular public/private key pair that is about to expire.

An issuing CA, or an RA acting on behalf of the issuing CA, shall authenticate all re--key or 'renewal' requests in the same manner as the initial application pursuant to Section 3.2.

3.3.2 Identification and authentication for re-key after revocation

Where the information contained in a certificate has changed or there is a known or suspected compromise of the private key resulting in a revocation, the issuing CA or the RA on behalf of the issuing CA, shall authenticate a re-key (i.e., a new certificate request with a new key pair) in the same manner as for initial application pursuant to Section 3.2. An issuing CA or an RA acting on behalf of the issuing CA shall verify any change in the information contained in a certificate before that certificate is issued.

3.4 Identification and authentication of revocation request

An issuing CA or RA, acting on behalf of the issuing CA, shall authenticate a request for revocation of a certificate in similar manner as a certificate request. An issuing CA shall establish the process, in its CPS, by which it addresses such requests and the means by which it will establish the validity of the request. An issuing CA shall keep a record of the type and details of the revocation request including the identity and authentication of the requesting person and the reason for revocation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

A CA shall require that all procedures (outlined in section 3.1 of this CP) and security requirements with respect to an application for a certificate be set out in their respective CPS or the relevant Visa product and service security requirements documentation.

An application for a certificate does not oblige a CA to issue a certificate.

4.1.1 Who can submit a certificate application

A CA shall require that all Subscribers be an employee or agent of Visa, or Visa Regions, Visa Clients and their agents, as well as employees, merchants, and cardholders that have contractual agreements with Visa or its Clients and are bound to comply with Visa Inc By-Laws, Operating Regulations and policies.

Any Subscriber information shall be complete, validated and accurate with full disclosure of all required information in connection with a certificate request.

4.1.2 Enrollment process and responsibilities

Subscribers registering for a certificate from an issuing CA will be required to consent to a Subscribers Agreement or equivalent agreement; either at the time of registration or upon certificate acceptance.

4.2 Certificate application processing

A CA shall require that each application be accompanied by:

8. Proof of Subscriber identity appropriate for certificate being requested in accordance with the relevant procedure for that type of certificate and/or Visa product or service with which the certificate is intended to be used.
9. Proof of authorization for any requested certificate attributes if other than those allowed for the type of certificate being requested;
10. A signed Subscriber agreement or Visa product or service participation agreement documenting the applicable terms and conditions governing the applicant's use of the certificate, and
11. A properly formatted PKCS #10 certificate request, including the public key component of a key pair that has been generated in a crypto device (hardware or software) that is appropriate to the certificate being requested.

4.2.1 Performing identification and authentication functions

A CA or, associated RA on behalf of the CA, shall perform identification and authentication procedures to validate a certificate application.

4.2.2 Approval or rejection of certificate applications

An issuing CA shall notify a Subscriber, directly or through the associated RA that the CA has rejected or has accepted the certificate application, created a certificate, and provided the Subscriber with access to the certificate. The CA may provide access to the certificate through manual or automated processes.

4.2.3 Time to process certificate applications

There is no stipulation for the period of time between the receipt of a request for a certificate and the issuance of a certificate. Processing time of a certificate application will described in a CA's CPS.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

CAs issue certificates based on requests that are correctly and properly verified according to Section 3.2. The issuance, and delivery or publication of a certificate by a CA indicates a complete and final approval of the certificate application by the issuing CA.

4.3.2 Notification to subscriber by the CA of issuance of certificate

An issuing CA shall notify, directly or through the associated RA, a Subscriber that the CA has created a certificate, and provide the Subscriber with access to the certificate. The CA may deliver the certificate through manual or automated processes.

CAs shall make certificates data available to Subscribers or Relying Parties, as appropriate, in accordance with Sections 4.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Notification by an issuing CA to a Subscriber of the publishing of the Subscriber's certificate in a repository or confirmation of delivery of Subscriber's certificate shall indicate approval of the certificate and acceptance by both the CA and the Subscriber of the certificate. By accepting and using the certificate the Subscriber agrees to comply with the terms of any policies referenced within the certificate.

4.4.2 Publication of the certificate by the CA

A CA is responsible for repository and publication functions. An issuing CA shall publish certificates in a repository based on the certificate publishing practices of the issuing CA (as defined in the CPS), as well as revocation information concerning such certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

A CA, participating in this Visa InfoDelivery PKI, shall require that its certificate signing private key is used only to sign certificates and CRLs for use with production implementations of Visa products and services. A CA shall not transfer its private key from the CA platform on which it was generated to another CA platform (except for disaster recovery or load balancing purposes) unless it obtains prior permission from the Visa Inc. Cryptographic Review Board. A CA shall use commercially reasonable efforts to ensure that issued certificates and associated private and public key pairs of PKI personnel are used only for CA functions to access and operate CA applications

A CA must not sign certificates for cross-certification intent in accordance with Section 3.2.6.

Private keys used by an RA for authentication in order to operate the RA applications, if applicable, shall not be used for any other purpose.

The Subscriber shall only use certificates, issued by an issuing CA, and their associated key pairs for the purposes identified in this CP and the CA's CPS. Certificates and associated key pairs may only be used for production implementations of Visa applications and services. They may not be used in a test environment unless a variance is obtained from the CA prior to their use.

4.5.2 Relying party public key and certificate usage

Prior to using a Subscriber's certificate, a Relying Party should verify that the certificate is appropriate for the intended use.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificate renewal is the re-issuance of a certificate with a new validity date using the same public key corresponding to the same private key. Certificate renewal will only be permitted within a time range prior to certificate expiration, as defined in the CAs CPS.

A CA shall require that any procedures for the revocation and renewal of a certificate will conform to the relevant provisions of this CP and the issuing CA's CPS. These procedures will be expressly stated in the Subscriber Agreement, or any product or service related agreement outlining the terms and conditions of the certificate use.

In general, certificate renewal is not allowed for any Visa commercial PKI. Prior to the expiry of a public/private key pair and certificate, a new key pair and certificate request shall be required by an authorized individual of the Visa Region, Visa Client or their agents representing the particular public/private key pair that is about to expire. An issuing CA or an RA on behalf of the issuing CA shall authenticate all requests in the same manner as the initial application.

Exceptions to this policy whereby an existing key pair may be 'reused' to obtain another certificate for the same entity must be approved by the Visa Inc. Cryptographic Review Board as part of the application or CA approval process and shall only apply to the specific application (or CA) for which it is requested. If the requesting entity is a participating CA, this approval must accompany the certificate request. If the exception is to apply to an end entity, the approval must be documented during the application approval process. In all cases, certificate renewal will only be permitted within 90 days prior to certificate expiration

4.6.2 Who may request renewal

A CA shall require that a Subscriber is currently in possession of a valid certificate and that the Subscriber remains an employee or agent of Visa, or Visa Regions, Visa Clients and their agents, as well as employees, merchants, and cardholders that have contractual agreements with Visa or its Clients and are bound to comply with Visa Inc By-Laws, Operating Regulations and policies.

4.6.3 Processing certificate renewal requests

Individuals, as described in section 4.1, requesting for certificate renewal will be in possession of a valid certificate. The Subscriber shall be tightly bound to their public keys and the information submitted.

The procedures and requirements with respect to the renewal of a certificate are set out in the respective CA CPS.

4.6.4 Notification of new certificate issuance to subscriber

An issuing CA shall notify, directly or through the associated RA, a Subscriber that the CA has renewed a certificate, and provide the Subscriber with access to the certificate. The CA may deliver the certificate through manual or automated processes.

4.6.5 Conduct constituting acceptance of a renewal certificate

Notification by an issuing CA to a Subscriber of the publishing of the Subscriber's certificate in a repository or confirmation of delivery of Subscriber's certificate shall indicate approval of the certificate and acceptance by both the CA and the Subscriber of the certificate renewal. By accepting and using the renewed certificate the Subscriber agrees to comply with the terms of any policies referenced within the certificate.

4.6.6 Publication of the renewal certificate by the CA

A CA is responsible for repository and publication functions. An issuing CA shall publish renewed certificates, as per the initial enrollment, in a repository based on the certificate publishing practices of the issuing CA.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Routine re-key is not supported. Prior to the expiry of a public/private key pair, a new certificate request using a new key pair shall be submitted by an authorized individual of the Visa Region, Visa Client or their agents representing the particular public/private key pair that is about to expire.

A CA or RA, on behalf of the issuing CA, shall authenticate all requests in the same manner as the initial application.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

A certificate may be modified:

12. At the CAs discretion, when the basis for any information in the certificate changes.
13. A change in the business relationship under which the certificate was issued occurs.

The issuing CA may revoke a certificate at any time if the issuing CA suspects that conditions may lead to a compromise of a Subscriber's keys or certificates.

4.8.2 Who may request certificate modification

A CA shall require that a Subscriber is currently in possession of a valid certificate and that the Subscriber remains an employee or agent of Visa, or Visa Regions, Visa Clients and their agents, as well as employees, merchants, and cardholders that have contractual agreements with Visa or its Clients and are bound to comply with Visa Inc By-Laws, Operating Regulations and policies.

The issuing CAs CPS will identify who can request for a certificate to be modified.

4.8.3 Processing certificate modification requests

Individuals, as described in section 4.1, requesting for certificate Modification will be in possession of a valid certificate. The Subscriber shall be tightly bound to their public keys and the information submitted.

The procedures and requirements with respect to the modification of a certificate are set out in the respective CA CPS.

4.8.4 Notification of new certificate issuance to subscriber

An issuing CA shall notify, directly or through the associated RA, a Subscriber that the CA has modified a certificate, and provide the Subscriber with access to the certificate. The CA may deliver the certificate through manual or automated processes.

4.8.5 Conduct constituting acceptance of modified certificate

Notification by an issuing CA to a Subscriber of the publishing of the Subscriber's certificate in a repository or confirmation of delivery of Subscriber's certificate shall indicate approval of the certificate and acceptance by both the CA and the Subscriber of the certificate Modification. By accepting and using the modified certificate the Subscriber agrees to comply with the terms of any policies referenced within the certificate

.

4.8.6 Publication of the modified certificate by the CA

A CA is responsible for repository and publication functions. An issuing CA shall publish modified certificates, as per the initial enrollment, in a repository based on the certificate publishing practices of the issuing CA.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate shall be revoked or otherwise invalidated:

1. When a Subscriber fails to comply with obligations set out in this Visa InfoDelivery PKI CP, the CA's CPS, the Visa Inc By-laws, Operating Regulations and policies, Subscriber agreement or applicable law.
2. When the basis for any information in the certificate changes;
3. A change in the business relationship under which the certificate was issued occurs.
4. When a Subscriber is no longer participating in the Visa product or service for which the certificate was issued.
5. Upon suspected or known compromise of the private key or the media holding the key;
6. Upon termination of a Subscriber; or
7. When a Subscriber no longer needs access to secured Visa resources.

The issuing CA may revoke a certificate at any time if the issuing CA suspects that conditions may lead to a compromise of a Subscriber's keys or certificates.

4.9.2 Who can request revocation

The revocation of a certificate shall only be requested by:

14. The Subscriber to whom the certificate is issued;
15. An authorized supervisor or manager on behalf of a Subscriber;
16. The authorized individual or organization that made the application for the certificate on behalf of a Visa organization, device or application;
17. The Visa entity on whose behalf an agent is operating (in the case of a certificate issued to an agent of the Visa Brand or a Visa Region or Client).
18. The issuing CA; or
19. An RA associated with the issuing CA.

4.9.3 Procedures for revocation request

CAs shall make certificate revocation data available to Subscribers or Relying Parties, as appropriate. The issuing CA will notify a Subscriber when a certificate bearing a Subscriber's identity is issued or revoked.

The CA will provide notice of revocation of a certificate that will be posted to the CRL or OCSP responder (if supported by the CA and the Relying Party's applications) within the time limits stated in Sections 4.9. The address of the CRL or OCSP responder shall be defined in the certificate.

The procedures and requirements with respect to the revocation of a certificate are set out in the respective CA's CPS. All requests for revocation shall be submitted to the issuing CA or RA on behalf of the CA, in writing (e.g., letter or email) and authenticated in a same manner as the initial certificate application. The authenticated revocation request and any resulting actions taken by the CA shall be recorded and retained as required. In the case where a certificate is revoked, justification for the revocation shall also be documented.

Where a Subscriber certificate is revoked, the revocation shall be published via the appropriate CRL or other commonly implemented certificate status publication method such as OCSP (if supported by relying party applications); of the issuing CA.

4.9.4 Revocation request grace period

The revocation grace period is the maximum period available, within which the Subscriber must make a revocation request to the issuing CA or RA acting on behalf of the issuing CA. The revocation request grace period shall be defined in the associated CA's CPS. The issuing CA may, at its discretion, suspend the affected certificate immediately upon notification pending authentication of the revocation request; this would enable the issuing CA to avoid a potentially unnecessary or unwarranted revocation.

4.9.5 Time within which CA must process the revocation request

The time within which a CA must process a revocation request shall be defined in the associated CAs CPS. The grace period shall not extend beyond 8 business hours from the time of discovery of a circumstance that would be a basis of revocation (see Section 4.9.1).

4.9.6 Revocation checking requirement for relying parties

It is the Relying Parties responsibility to check the status of all certificates in the certificate validation chain against current CRLs or the OCSP responder (whichever is referenced in the certificate) prior to their use. If the Relying party caches the CRL, it must retrieve a 'fresh' CRL daily A Relying Party must also verify the authenticity and integrity of CRLs or the OCSP signer.

4.9.7 CRL issuance frequency

A CA must publish up-to-date certificate status information by commonly supported methods such as CRL or OCSP responder.

If CRLs are used, a CA shall issue an up-to-date CRL to attest the most current certificate status of all issued certificates. The CRL issuance frequency will be specified in the CA's CPS. At a minimum, an offline CA shall publish a CRL at least monthly. (The one exception to this is the Visa InfoDelivery Root CA that shall issue a CRL at least annually). Online CAs must publish CRLs more frequently, at least daily. A CA shall synchronize, automatically or manually, its CRL issuance with an accessible directory or web site to provide accessibility of the most recent CRL to Relying Parties.

4.9.8 Maximum latency for CRLs

A CA shall synchronize, automatically or manually, its CRL issuance with an accessible directory or web site to provide accessibility of the most recent CRL to Relying Parties. The maximum latency period shall be defined in the associated CAs CPS.

4.9.9 On-Line revocation/status checking availability

On line certificate revocation status checking may be supported via Online Certificate Status Protocol (OCSP). If OCSP is implemented, the OCSP Responder shall be available for a high percentage of each 24-hour period. The OCSP availability requirements will be specified in the CA's CPS.

4.9.10 On-Line revocation/status checking requirements

If OCSP is implemented, applications must support OCSP as specified in IETF RFC 2560 and its successors. The CA or an OCSP signer, that possesses a certificate signed by the CA, shall digitally sign all OCSP responses.

4.9.11 Other forms of revocation advertisements available

No Stipulation.

4.9.12 Special requirements re-key compromise

No stipulation.

4.9.13 Circumstances for suspension

A certificate must be suspended or revoked whenever any of the conditions listed in Section 4.9.1 are suspected or known. An issuing CA may, at its discretion, suspend a certificate rather than revoking it immediately pending validation of the revocation request. During the suspension period, the suspended certificate shall be listed on the issuing CA's CRLs as 'on hold' and treated by Relying Parties as revoked. Suspensions shall last until the revocation or suspension request is successfully authenticated and the issuing CA can determine whether the certificate will be revoked or reinstated.

4.9.14 Who can request suspension

Any of the parties listed in Section 4.9.2 may request suspension.

4.9.15 Procedure for suspension request

The procedures and requirements with respect to the suspension of a certificate are set out in the respective issuing CA's CPS. All requests for suspension shall be submitted to the issuing CA or RA on behalf of the CA, in writing (e.g., letter or email) and authenticated in a same manner as the initial certificate application. A certificate may be suspended pending resolution of outstanding items that could be a basis for revocation. The authenticated suspension request and any resulting actions taken by the CA shall be recorded and retained as required.

4.9.16 Limits on suspension period

If a certificate is suspended in response to a suspension request, the minimum period of suspension should be until a documented analysis of appropriate next steps occurs. If a certificate is suspended pending verification of a revocation request, the suspension period shall be appropriate to the period needed to validate the revocation request. Suspension period limits shall be defined in the associated CA's CPS. At the end of the suspension period, the issuing CA shall make a determination regarding whether the certificate will be reinstated, revoked or the suspension period extended.

4.10 Certificate status services

4.10.1 Operational characteristics

Characteristics to be specified in the CA's CPS.

4.10.2 Service availability

Requirements will be specified in the CA's CPS.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

The end of a subscription as a result of no longer requiring the service, compromise, or termination of employment (voluntary or imposed) will result in the immediate revocation of the certificate and the publishing of a CRL or other certificate status verification system.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

CA Private Signing Key(s) shall not be escrowed.

Subscriber private keys:

SIGNATURE

Digital Signature private keys shall not be escrowed.

CONFIDENTIAL

Private confidentiality keys may be escrowed.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

. Subscribers, in particular Visa Regions, MembersClients, and their agents, shall satisfy the security requirements as documented in the relevant Visa product and service documentation prior to certificate issuance.

Of critical importance, Visa Regions and MembersClients, and their agents shall provide the necessary protection to their private keys when or when not in use. It is required that CA signing keys and keys used to protect those keys be generated in and protected by a secure cryptographic hardware module. Private and secret keys must not be in human comprehensible form to any person at any time.

Subscribers who are subordinate or participating CAs shall provide the physical security controls outlined in Sections 5.1.1 to 5.1.8.

Other Subscribers, such as workstations, servers or devices, that contain private keys on a hard drive (software generated) shall be physically secured or protected with an appropriate boot level or suitable two-factor authentication access control.

5.1.1 Site location and construction

In addition to the provisions described regarding the CA documentation, the following requirements and procedures are to be implemented:

20. The access control systems must be:

- Inspected at least quarterly by qualified personnel
- Documented with the documentation retained for at least a one year period.

21. All access control and monitoring systems must be tied to a UPS. The UPS system must be inspected:

- At least annually
- Documented with the documentation retained for at least a one year period.

5.1.2 Physical access

As per *visa security requirements for secure areas*

5.1.3 Power and air conditioning

A CA must ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water exposures

A CA must ensure that the CA system is protected from water exposure.

5.1.5 Fire prevention and protection

A CA must ensure that the CA system is protected with a fire suppression system.

5.1.6 Media storage

A CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

5.1.7 Waste disposal

A CA must ensure the sanitization or destruction of all confidential media before release for disposal.

5.1.8 Off-site backup

A CA must ensure that facilities used for off-site back up have the same level of security as the primary CA site.

5.2 Procedural controls

5.2.1 Trusted roles

5.2.1.1 CA trusted roles

A CA **shall** require a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection. PKI personnel access to the CA system(s) is to be limited to those actions they are required to perform in fulfilling their responsibilities.

These responsibilities shall be well understood by the CA personnel.

There is a separation of duties and two-person control required for specific activities, such as:

- Generation of a new key pair;
- Replacement of the CA private signing key and associated certificate;
- Change in the certificate profile security policy (e.g. renewal)

All CA/RA Administrators and RA/vettors will be individually accountable for their actions. This will be accomplished by a combination of physical, electronic and policy controls:

- Restricted access to the facility - entry is monitored for both entry and exit
- Audit logs will record administrator log-on and log-out of the operating system
- Audit logs will record administrator log-in and log-out of the CA application
- Audit logs will record certificate creation, revocation, etc. (see section 5.4)
- Technical controls that enforce dual access
- Policy and procedural controls that require dual access

5.2.1.2 RA trusted roles

A CA shall require that RA personnel understand their responsibility for the identification and authentication of prospective Subscribers and perform the following functions:

22. Acceptance of certificate requests, certificate changes, certificate revocation requests and key recovery requests (if applicable);
23. Verification of a Subscriber's identity and authorizations;
24. Verification that any pre-requisites that must be performed prior to the generation of the key pair and certificate request have been successfully completed (e.g., product participation agreement, security audit)
25. Secure transmission of applicant information to the issuing CA; and
26. Provision of shared secrets, as required, for authenticating Subscribers.

5.2.2 Number of persons required per task

A CA shall provide the proper security and procedures such that no single individual shall perform CA activities (e.g., generation or loading of cryptographic keys, CA/RA application system configuration changes). This practice is referred to as split knowledge and dual control[1]. Access

[1] As defined in ISO 9564-1, split knowledge is "a condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key". The resultant key exists only within "secure cryptographic devices". Dual control is explained in the standard as "a process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key".

to other CA/RA configuration components may be performed under single control as long as compensating controls are identified and followed.

Multi-user control is required for CA key generation as outlined in Section 6.2.2.

CAs must have a verification process that provides an oversight of all activities performed by privileged CA role holders. That is roles that can issue certificates, generate keys and administer the CA configuration settings.

5.2.3 Identification and authentication for each role

All CA Personnel shall have their identity and authorization verified before they are:

27. Included on the access list for a CA facility;
28. Included on the access list for logical access to the CA system; or
29. Given a certificate for the performance of their CA operation's role; Each of these certificates and accounts (with the exception of the CA signing certificates) shall:
    - Be directly attributable to an individual;
    - Not be shared; and
    - Be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls.

CA operations shall be secured, using commercially reasonable mechanisms such as token based strong authentication and encryption (i.e., smart cards).

5.2.4 Roles requiring separation of duties

A CA shall require a separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection.

5.3 Personnel controls

A CA shall require that all personnel performing duties with respect to the operation of a CA (e.g., CA or RA administrators, key custodians and RA/vettors) shall:

30. Be bound by the terms and conditions of the position they are to fill;
31. Have received comprehensive training with respect to the duties they are to perform;
32. Be bound by contract or statute not to disclose sensitive CA security-relevant information or Subscriber information; and
33. Not be assigned duties that will cause conflict with their CA duties.

5.3.1 Qualifications, experience, and clearance requirements

A CA shall require that all personnel performing duties with respect to the operation of a CA have sufficient qualification and experience in PKI. All personnel shall meet Visa Inc. personnel security requirements.

5.3.2 Background check procedures

Background checks shall be performed on all CA operations personnel in accordance with Visa Inc. Operating Regulations and any relevant country legal restrictions. All PKI personnel considered for employment shall be thoroughly screened by a reputable investigative agency:

- Complete criminal background verification;
- Complete and verifiable employment history

Such screening should be repeated on an annual basis to verify the continued trustworthiness of these individuals.

5.3.3 Training requirements

A CA shall provide comprehensive training for all PKI personnel performing duties with respect to the operation of the CA. The CA shall outline the training requirements in its CPS.

5.3.4 Retraining frequency and requirements

The requirements for Section 5.3.3 shall be kept current to accommodate changes in a CA system (software and procedures). Refresher training shall be conducted as required, and management shall review these requirements once a year.

5.3.5 Job rotation

No Stipulation

5.3.6 Sanctions for unauthorized actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of a CA, that CA must revoke the person's access to the CA system immediately. A CA may revoke a certificate when an entity fails to comply with obligations set out in this Visa InfoDelivery PKI CP, its CPS, Visa Inc By-Laws, Operating Regulations, and policies. A CA may revoke a certificate at any time if a CA suspects that conditions may lead to a compromise of keys or certificates.

5.3.7 Independent contractor requirements

A CA shall limit contractor access to the CA facility in accordance with the provisions in the *Visa Key Controls* described in the section on personnel controls..

5.3.8 Documentation supplied to personnel

This Visa PKI shall make all CAs, within the Visa InfoDelivery PKI hierarchy, and their personnel aware of the requirements of applicable CP, CPS and any other specific policies, procedures, documents, and/or contracts relevant to their particular job requirements.

5.4 Audit logging procedures

5.4.1 Types of events recorded

A CA shall record in audit log files all relevant events, successes and failures, relating to the security of that CA system. All relevant logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity which caused the event.

A CA shall indicate in its CPS what information is logged. All relevant agreements and correspondence should be collected and consolidated either electronically or manually in one single location to facilitate decision-making.

CA Physical Security Logs

CA physical access is a primary concern and access events must be recorded to the following criteria:

34. Automated mechanisms must exist for logging access.
35. All access granting, revocation, and review procedures must be documented.
36. Visitors (contractors, maintenance personnel, etc.) to the physically secure environments must be escorted and sign an access logbook. This log must be maintained within the physically secure facility. This logbook must include:
    - Date and time in/out,
    - Name and signature of visitor,

- Affiliation of visitor,
- Name and signature of individual escorting the visitor,
- Reason for visit.

37. All alarm events must be documented. Under no circumstances shall an individual sign-off on an alarm event in which they were involved.

38. The use of any emergency entry or exit mechanism must cause an alarm event. An assessment must occur within twenty-four hours to identify the effect (e.g., loss of dual control by authorized individuals) of the use of this mechanism. This assessment must be documented and retained for at least a one year period.

39. A process must exist for synchronizing the time and date stamps of the access, intrusion detection and monitoring (camera) systems to ensure the accuracy of the logs. This may be done by either automated or manual mechanisms. If a non-continuous process is utilized, then the process must occur at least quarterly. Documentation of the synchronization must be retained for at least a one-year period.

5.4.2 Frequency of processing log

The frequency of audit log reviews will be based on the security requirements of a CA. At a minimum, a review shall be conducted once every 30 days. Online systems shall have reviews conducted at least weekly. All significant events shall be explained in an audit log summary. Actions taken following these reviews shall be documented. The events logged, and the associated actions taken, shall be documented in the CPS.

5.4.3 Retention period for audit log

A CA shall retain its audit logs (for both CA and RA systems) for records pertaining to the issuance and any revocation of a certificate, for at least seven years after the certificate is revoked or expired. Time lines for retention of other audit records must conform to standard commercial and legal requirements. A CA shall retain audit logs in a manner described in Section 5.5.2.

5.4.4 Protection of audit log

An electronic audit log system shall include mechanisms to protect the log files from unauthorized viewing, modification or deletion.

Manual audit information shall be physically protected from unauthorized viewing, modification or deletion.

5.4.5 Audit log backup procedures

Audit logs and audit summaries shall be backed up or copied daily (for offline CAs this must occur after every ceremony). Alternatively, backups may be performed more frequently (e.g., each time the CP has accessed its database). Time lines for retention of backups shall conform to standard commercial and legal requirements. At a minimum, backups must be retained for a seven-year period for records pertaining to the issuance and/or revocation of a certificate, after the certificate is revoked or expired.

5.4.6 Audit collection system (internal vs. external)

A CA shall identify their audit collection system(s) (manual and/or automated) in their CPS.

5.4.7 Notification to event-causing subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual or entity that caused the event.

5.4.8 Vulnerability assessments

Events in the audit process are logged, in part, to monitor inappropriate behavior, system vulnerabilities and/or compromises. A CA shall perform a vulnerability assessment and take action taken, as required, following an examination of these monitored events.

5.5 Records archival

Public verification keys contained in digital certificates, confidentiality private keys stored by the issuing CA, CRLs, and any other information generated by the issuing CA shall be retained for a minimum of seven (7) years after the expiry of the key material. This requirement does not include the backup of private signature keys.

5.5.1 Types of records archived

The following information must be archived:

- Public verification keys contained in digital certificates, CRLs, and any other information generated by the issuing CA,
- Visa Region and Client Subscriber agreements,
- Any other contracts or agreements associated with the Visa InfoDelivery CAs, and
- Audit results.

5.5.2 Retention period for archive

Audit information, Subscriber agreements and any identification and authentication information shall be retained for the length of time identified in the CA's CPS.

5.5.3 Protection of archive

Archived information shall include mechanisms to protect the log files from unauthorized viewing, modification or deletion.

Manual archived information shall be physically protected from unauthorized viewing, modification or deletion.

5.5.4 Archive backup procedures

If key recovery is implemented, data encryption private keys (used for decryption purposes) that are backed up by the issuing CA are to be protected at a level of physical and cryptographic protection equal to or exceeding that in place at the issuing CA site.

A second copy of all material retained or backed up must be stored in a location other than the issuing CA site and shall be protected either by physical security alone or a combination of physical and cryptographic protection. Any such secondary site shall provide adequate protection from environmental threats such as temperature, humidity, and magnetism.

5.5.5 Requirements for time-stamping of records

All documents archived pursuant to this section shall be permanently marked with the date of their creation or execution.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

A CA shall verify periodically the integrity of the archives both on site and stored off-site. The frequency of this verification will be stipulated in the CA CPS.

5.6 Key changeover

If a key changeover is required for a CA (e.g., due to expiration), the CA shall generate a new key pair and submit the certificate request to the issuing CA for signature. The old CA key pair shall be removed from the CA and destroyed. There shall be a key changeover period where the CA phases out the previous CA private key and public certificate. Any CA private key shall not be used to issue certificates with an expiration date that exceeds the expiration date of the CA certificate associated with that private key.

When a certificate expires or is compromised, a new key pair shall be generated and submitted to the issuing CA with the request for replacement of the certificate. The expired or compromised key pairs shall be removed from the entity and destroyed by an authorized person. Where a Subscriber's certificate has been revoked as a result of non-compliance, the issuing CA or an RA on behalf of the issuing CA shall verify that the reasons for non-compliance have been addressed to the issuing CA's satisfaction prior to certificate re-issuance.

Subscribers (end entity or CA) may apply for a new certificate within three (3) months prior to the expiration of their existing certificate providing the current certificate has not been revoked.

Any exception to this policy whereby an existing key pair may be 'reused' to obtain another certificate for the same entity must be approved in writing by the Visa Inc. Cryptographic Review Board and shall only apply to the specific instance (e.g., application or CA) for which it is requested. This approval must accompany the certificate request.

5.7 Compromise and disaster recovery

Information pertaining to disaster recovery of the Visa InfoDelivery CAs will be provided in the appropriate CPS and further detailed in the Disaster Recovery Plan for each CA.

In the unlikely event that there is a compromise of a CA key with the Visa InfoDelivery CAs or participating CAs, the CA shall notify its Subscribers promptly. Detailed instructions will be specified in the respective CA's CPS.

In the unlikely event that there is a compromise of a CA key with the Visa InfoDelivery CAs, all participating CAs will be notified promptly. Detailed instruction will be provided in the Visa InfoDelivery CA Operations Procedures, but key steps to be followed are:

- Notification of all sub CAs and customers;
- Revocation of all certificates associated with the compromised keys as deemed necessary;
- Investigation of the compromise;
- Reporting results of the investigation and required actions;
- Implementation of actions.
- Key ceremonies (for all required CAs);
- Issuance of new certificates as deemed necessary.

5.7.1 Incident and compromise handling procedures

Incident and comprise handling procedures will be provided in the Visa InfoDelivery CA Operations Procedures.

5.7.2 Computing resources, software, and/or data are corrupted

A participating CA shall provide business continuity procedures in its CPS and Disaster Recovery Plan that outline the steps to be taken in the event of corruption or loss of computing resources, software and/or data.

5.7.3 Entity private key compromise procedures

Subscribers must be notified as to procedures for dealing with suspected key compromise, certificate renewal, and service cancellation.

Subscriber (end entity) key compromise will result in immediate revocation. Re-issuance will be in accordance with section 3.3.2.

5.7.4 Business continuity capabilities after a disaster

A CA shall provide business continuity procedures in a Disaster Recovery Plan that outline the steps to be taken in the event of corruption or loss of computing resources, software and/or data.

5.8 CA or RA termination

In the event that a CA ceases operation, it shall notify the Visa Inc. Cryptographic Review Board and the CA's Subscribers of its intention to cease operation at least forty-five (45) days prior to termination of the service. Certificates issued by this CA may be retired (allowed to expire) where there is not any reasonable expectation of inappropriate usage of the certificate prior to the expiration date. Certificates must be revoked where there is potential for inappropriate usage. The CA shall arrange for the certificate files to be archived for seven years in case of disputes. Private keys used for signing a certificate or CRL or for creating a digital signature cannot be transferred. Details of these arrangements shall be specified in the individual CA's CPS.

In the event of a change in management of a CA's operation, that CA must notify all Subscribers for which it has issued certificates, and the Visa Inc. Cryptographic Review Board.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation shall be supported in either hardware or software as stipulated in section 6.1.6.

Key pairs must either be generated by the device which will use the key pair, or if generated externally, the key pair and all related critical security parameters (e.g., secret seeds) must be deleted (zeroized) immediately after the transfer to the device which will use the key pair occurs.

6.1.2 Private-key delivery to subscriber

Key pairs generated external to the device that uses the key pair must be securely transferred and loaded into the device and must provide for key protection in accordance with Section 6.2. That is, the secrecy of the private key and the integrity of the public key must be ensured.

6.1.3 Public-key delivery to certificate issuer

All Public-keys and certificates may be stored in the CA's repository and/or LDAP directory. Delivery of public keys shall be in DER encoded (binary or base64) PKCS #10 format

6.1.4 CA Public-key Delivery to Users

All Public-keys and certificates may be stored in the CA's repository and/or LDAP directory. The CA public key (as part of the certificate) shall be delivered to a Subscriber as part of the issuing process. The format must be DER encoded (binary or base64) or PKCS #7 (binary or base64), with or without chain, or PEM depending on the Subscriber's requirements and as outlined in the issuing CA's CPS.

6.1.5 Key sizes

A CA shall require that the key pairs for all PKI entities be a minimum of 1024 bits in length and use the RSA algorithm for the key algorithm.

6.1.6 Public key parameters generation and quality checking

All CA Signature keys shall be generated using a random or pseudo-random process as described in ISO 9564-1 and ISO 11568-5 that is capable of satisfying the statistical tests as defined in NIST Special Publication 800-22. CA private keys are to be protected by a secure cryptographic hardware module rated at FIPS 140-2, Level 3 or higher.

End entity key pairs for Visa Regions and Clients or their agents, destined for use with Visa products and services must be generated and protected as detailed in the relevant Visa product and service documentation. At a minimum, the key generation requirements must meet the business objectives of the Visa product and service.

Key pairs for all other entities may be generated and stored in software or protected by secure cryptographic hardware modules as defined by the issuing CA practices as documented in their respective CPS.

6.1.7 Key usage purposes (as per X.509v3 key usage field)

The CA's certificate signing private keys shall be used only for signing Subscriber (individual, organization, device/application and subordinate CA, where applicable) certificates, and CRLs. The key usage shall be set for key certificate signing and CRL signing.

SIGNATURE

Keys may be used for client authentication and message integrity. They may also be used for session key establishment. The certificate KeyUsage field must be used in accordance with the IETF PKIX Certificate and CRL Profile. The following KeyUsage value must be present in all end entity certificates used for the aforementioned security services:

DigitalSignature

CONFIDENTIAL

Keys may be used for exchange and establishment of keys used for session and data confidentiality. The certificate KeyUsage field must be used in accordance with the IETF PKIX Certificate and CRL Profile. The following KeyUsage value must be present in all end entity certificates used for the aforementioned security services:

KeyEncipherment;

KeyAgreement and / or

DataEncipherment

In some cases a CA may also employ private keys for message integrity and encryption; these keys must be separate from the certificate and CRL signing keys.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The Subscriber shall protect its private key from disclosure according to the requirements as defined by the issuing CA's CPS. The Subscriber is responsible for its private keys. Subscribers shall change their passwords in accordance with the security policy of the relevant Visa organization or Clients. Private keys shall only be used for the intended purpose, unless otherwise granted by the Issuing CA of the corresponding certificate.

The private key of an entity shall be protected from unauthorized use by a combination of commercially reasonable cryptographic and physical access control mechanisms as defined by the issuing CA and detailed in their CPS. The level of protection must be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism must include a facility to temporarily lock the account after a predetermined number of login attempts.

CA personnel shall require that CA signing keys and private keys issued to them for CA administrative function be protected in accordance with Sections 4 and 6.

6.2.1 Cryptographic module standards and controls

All CA (Visa InfoDelivery CAs and participating CAs) digital signature key generation, CA digital signature key storage and certificate signing operations shall be performed in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance. All other CA cryptographic operations shall be performed in a cryptographic module validated to at least FIPS 140-2 Level 1 (software module) or otherwise verified to an equivalent level of functionality.

Key pairs for Visa Regions and Clients or their agents, destined for Visa products and services shall be generated and protected as detailed in the relevant Visa product and service documentation. It is recommended that keys be generated in and protected by a secure cryptographic hardware module. At a minimum, the key generation and protection requirements must meet the business objectives of the Visa product and service.

Other Subscribers shall use cryptographic modules validated to at least FIPS 140-2 Level 1 or equivalent software cryptographic modules, at the discretion of the issuing / participating CA as documented in their respective CPS and as detailed in the relevant Visa product and service documentation.

6.2.2 Private Key (n out of m) multi-person control

There shall be multiple-person control for CA key generation operations. At a minimum, there shall be multi-person control for operational procedures such that no one person can gain control over the CA signing key. The principle of split knowledge and dual control as defined in Section 5.2.2 shall be applied.

6.2.3 Private key escrow

CA Private Signing Key(s) shall not be escrowed.

Subscriber private keys:

SIGNATURE

Digital Signature private keys shall not be escrowed.

CONFIDENTIAL

Private confidentiality keys may be escrowed.

6.2.4 Private key back-up

The Visa InfoDelivery CAs and participating CAs shall back up CA private signing keys in a secure manner to support disaster recovery operations.

Subscribers are responsible for backing up the private key associated with the certificate used in conjunction with a Visa product or service in a secure manner (e.g., locked cabinet, safe).

Participating CAs may back up all private confidentiality keys that the CA issues dependent on Visa specific business requirements.

6.2.5 Private key archival

Refer to Section 5.5.

6.2.6 Private Key transfer into or from a cryptographic module

No stipulation

6.2.7 Private Key storage on cryptographic module

CA digital signature key storage shall be kept on a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3 or higher.

6.2.8 Method of activating private key

The Entity must be authenticated to the cryptographic module before the activation of the private key. This authentication, at a minimum will be in the form of a password. When deactivated, private keys must be kept in encrypted form only.

6.2.9 Method of deactivating private key

When keys are deactivated the application must clear the keys from memory before the memory is de-allocated. Any disk space where keys were stored must be over-written before the space is released to the operating system. The cryptographic module must automatically deactivate the private key after a pre-set period of inactivity.

6.2.10 Method of destroying private key

Upon termination of use of a private key, over-writing must securely destroy all copies of the private key in computer memory and shared disk space. Private key destruction procedures must be described in the CPS.

6.2.11 Cryptographic Module Rating

All CA digital signature key generation, CA digital signature key storage and certificate signing operations shall be performed in a secure cryptographic hardware module rated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance.

6.3 Other aspects of key pair management

6.3.1 Public key archive

The issuing CA shall retain all verification public keys for the period of time defined in its CPS.

6.3.2 Certificate operational periods and key pair usage periods

In all cases, a participating CA private signing key shall expire no later than the Visa InfoDelivery CA key that signed the participating CA public verification key. If the CA certificate contains a private key usage extension, the expiration date for the private signing key shall correspond to the date included in that extension.

Subscriber keys shall have a validity period appropriate to the intended use of the certificate as described in the relevant Visa product and/or service documentation. Non-CA Subscriber keys and certificates shall expire prior to the issuing CA key that signed the Subscriber's public verification key.

6.4 Activation data

6.4.1 Activation data generation and installation

If activation data is used it shall be unique and unpredictable.

6.4.2 Activation data protection

If activation data is used, it shall be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms..

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Computer security controls for CAs must provide protection from unauthorized access, modification, substitution, insertion and deletion. These controls will provide protection to help ensure that any such attempts will be prevented or will have a high probability of being detected in a timely manner. The following functionality, for the Visa InfoDelivery CAs and participating CAs, shall be provided by the operating system, or through a combination of operating system, CA software, and/or physical safeguards (policies and procedures). Each CA server must include the following functionality:

40. Logical access control to CA services;
41. Enforced separation of duties for CA administrative roles;
42. Identification and authentication of CA administrative roles and associated identities;
43. Use of cryptography for session communication and database security;
44. Archival of CA and end entity history and audit data;
45. Audit of security related events;
46. Trusted path for identification of PKI roles and associated identities; and
47. Recovery mechanisms for keys and CA system.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

All CAs must use CA software that has been designed and developed under a documented development methodology. An integrity verification process to influence security safeguard design and minimize residual risk must support the design and development process.

6.6.2 Security management controls

A formal configuration management methodology shall be used for the installation and ongoing maintenance of a CA system. CA software, when first loaded shall provide a method for a CA to verify that the software on the system:

- Originated from the software developer;
- Has not been modified prior to installation; and
- Is the intended version.

A CA shall provide a commercially reasonable mechanism to periodically verify the integrity of the software.

A CA shall have commercially reasonable mechanisms and policies in place to control and monitor the configuration of the CA system.

Upon installation and at least once per quarter the integrity of the CA system should be validated.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

The Visa InfoDelivery Root CA is not connected to a network outside of it's domain, and therefore eliminates any threat of attack through open or general-purpose networks.

Visa Inc.Inc Brand CAs and participating CAs, if connected to a public network and supporting Visa products and services shall use commercially reasonable efforts to protect its servers from attack through any open or general purpose network with which it is connected. Such protection shall be provided though a combination of hardware and/or software (firewalls and network monitoring) configured to allow only the protocols and commands required for the operation of the CA and the Visa product or service.

A CA shall define those protocols and commands required for the protection of the CA in its CPS or other procedural documents.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

Visa InfoDelivery CAs and participating CAs shall issue X.509 Version 3 end entity and CA certificates based upon the IETF PKIX Certificate and CRL Profile (RFC 3280 and its successors) for use with Visa products and services (corporate and commercial). . The PKI end entity software shall support all the base (non-extension) X.509 fields as well as any certificate extensions defined in the issuing CA's CPS.

The Base Certificate Format will conform to the X.509 standard.

7.1.2 Certificate extensions

The Visa InfoDelivery PKI will support version 3 extensions in accordance with RFC 3280 'Internet X.509 Public Key Infrastructure Certificate and CRL Profile' dated April 2002 and its successors. All extensions used by the Visa InfoDelivery CA, participating CAs and its Subscribers shall be published in their respective CPS.

7.1.3 Algorithm object identifiers

The Visa InfoDelivery CA and participating CAs shall use, and Subscribers and Relying Parties shall support, for signing and verification, the following:

48. RSA (1024 bits modulus or higher) algorithm in accordance with PKCS#1; and
49. SHA-1 algorithm in accordance with FIPS PUB 180-1 and ANSI X9.30 part2

7.1.4 Name forms

Every DN must be in the form of an X.501 DirectoryString.

7.1.5 Name constraints

Subject and Issuer DNs must comply with PKIX standards and be present in all certificates.

7.1.6 Certificate policy object identifier

A CA shall have the Policy OID contained within the certificates it issues.

7.1.7 Usage of Policy Constraints extension

A CA may populate and mark as critical the policyConstraints extension.

7.1.8 Policy qualifiers syntax and semantics

A CA may populate the CertificatePolicies extension with the OID identifier and policyQualifiers containing the URL of its CPS. User Notice Qualifier which point to an applicable Relying Party Agreement may be used at the discretion of the issuing CA.

7.1.9 Processing semantics for the critical Certificate Policies extension

Critical extensions shall be interpreted as defined in PKIX.

7.2 CRL Profile

7.2.1 Version number

Visa InfoDelivery CAs and participating CAs shall issue X.509 version 2 CRLs in accordance with the RFC 3280 'Internet X.509 Public Key Infrastructure Certificate and CRL Profile' dated April

2002 and its successors. The CRLs must be published on a repository and /or an OCSP responder. The Subscriber and Relying Party software shall support all of the base (non-extension) X.509 fields.

7.2.2 CRL and CRL entry extensions

The CA CPS shall define the use of any extensions supported by the CA, RA, Subscribers and Relying Parties.

7.3 OCSP Profile

7.3.1 Version number(s)

A CA's OCSP responders (if supported) will implement Version 1 of the OCSP specification as defined by RFC2560 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol), with the exception of including nonce as one of the requestExtensions in requests.

7.3.2 OCSP extensions

A CA may support On-line Certificate Status Protocol (OCSP) via an OCSP responder. The CA CPS shall define the use of any extensions supported by the CA, RA, Subscribers and Relying Parties. The OCSP responder may be 'populated' directly by the CA or via CRLs issued by the CA.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

A compliance audit provides an independent third party certification that the CA is operating as stated in this CP and the CA's CPS.

8.1.1 Visa InfoDelivery CA (X.509) and offline Brand CAs

The Visa InfoDelivery Root CA (X.509) and offline Brand CAs shall have a compliance audit performed annually, at its expense, as part of a WebTrust Certification Authority assessment. The annual compliance audit will determine whether the Visa InfoDelivery CA performance (business practices and controls) meets the requirements of this CP, the standards established in its CPS, and the conformity with American Institute of Certified Public Accountants/ Canadian Institute of Chartered Accountants (AICPA/CICA) WebTrust principles and criteria.

8.1.2 Participating CAs and online Brand CAs

Participating CAs and online Brand CAs must have a compliance audit performed at least annually, at their expense, to demonstrate compliance with the Visa InfoDelivery PKI CP, and participating CA's CPS. The Visa X.509 Policy Authority Inc. Cryptographic Review Board reserves the right to request a compliance audit on a more frequent basis. At the discretion of the Visa Inc. Cryptographic Review Board or a field review conducted by a qualified third party approved by the Visa X.509 Policy AuthorityInc. Cryptographic Review Board. Participating CAs must notify the Visa Inc. Cryptographic Review Board of any material changes in the operation of its CA system (e.g., change in location or management, change in CA system platform). If requested, the CA must undergo an audit to verify that the CA is still in compliance with this CP.

A copy of the compliance audit report shall be submitted to the Visa Inc. Cryptographic Review Board.

The Visa Inc. Cryptographic Review Board reserves the right to verify that a compliance audit has been performed and that the participating CA has complied with the requirements of this CP.

8.2 Identity/qualifications of assessor

The compliance auditor must demonstrate competence in the field of PKI, logical and physical security and cryptographic key management. The auditor must be thoroughly familiar with the requirements that the Visa Inc. Cryptographic Review Board imposes on the issuance and management of all certificates by the CAs being audited. The compliance auditor should perform such compliance audits as a primary responsibility.

The compliance auditor must be a practitioner who is approved by the Visa Inc. Cryptographic Review Board to perform CA audits to verify and confirm compliance with this Visa InfoDelivery PKI CP.

8.3 Assessor's relationship to assessed entity

8.3.1 Visa InfoDelivery CA (X.509) and offline Brand CAs

The compliance auditor shall not have any financial, legal or conflicting business relationship with the Visa InfoDelivery CAs, which could otherwise result in a biased outcome.

8.3.2 Participating CAs and online Brand CAs

Where the audited party is a participating CA or online Brand CA, the compliance auditor must be an unbiased third party, with non-conflicting interests. The Visa Inc. Cryptographic Review Board must approve the compliance auditor.

8.4 Topics covered by assessment

The purpose of a compliance audit shall be to verify that an entity subject to the requirements of this CP is acting in accordance with these requirements. The compliance audit will cover all requirements that define the operation of a CA under this CP including:

50. CA business practices disclosure;

51. CA service integrity (key and certificate life cycle management) with respect to the Visa product or service; and

8.5 Actions taken as a result of deficiency

When a deficiency is noted, the following actions shall be taken:

52. The compliance auditor must note the deficiency as part of the report;

53. The compliance auditor may meet with the CA (or its certificate processor) and determine if the deficiency can be remedied. An action plan shall be developed and steps taken to remedy the deficiency.

54. The compliance auditor must report the deficiency to the Visa Inc. Cryptographic Review Board and if the Visa Inc. Cryptographic Review Board deems the deficiency to have risk to the operation and integrity of the Visa Inc. Cryptographic Review Board may refuse to issue a certificate to the CA or if a certificate has been issued to the CA, suspend or revoke it..

8.6 Communication of results

The compliance auditor shall provide Visa Inc. Cryptographic Review Board with a copy of the results of the compliance audit. The results will not be made public unless required by law.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The charging of fees is subject to the appropriate authority and policy of the issuing CA. Notice of any fee charged to a Subscriber or Relying Party shall be brought to the attention of that entity.

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

This section is not meant to replace the liability and indemnifications provisions of the Visa Inc.By-laws, Operating Regulations and policies, which shall continue to be enforced and in effect.

9.2.1 Insurance coverage

Visa InfoDelivery PKI and CAs within the Visa InfoDelivery PKI shall maintain, at its own expense, Commercial General Liability insurance with a sufficiently high limit for the conduct of its business. This requirement can be met with any combination of primary and umbrella policies. The insurance shall cover liability arising from premises, operations, independent contractors, products-completed operations, personal injury and advertising injury and liability assumed under an insured contract.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

Visa InfoDelivery PKI, Visa InfoDelivery CA or participating CA, is not a trustee, agent, fiduciary, or other representative of the Subscriber and the relationship between them is not that of an agent and/or a principal. Visa InfoDelivery PKI, Visa InfoDelivery CA or participating CA makes no representation to the contrary, either implicitly, explicitly, by appearance or otherwise. Subscribers do not have any authority to bind Visa InfoDelivery PKI, Visa InfoDelivery CA or participating CA by contract, agreement or otherwise, to any obligation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Subscriber information not appearing in certificates and in public directories held by a CA, or an associated RA (e.g. registration and revocation information, logged events, and correspondence

between Subscriber and CA) is considered confidential and shall not be disclosed by the CA unless required by law or otherwise in accordance with the CA's applicable policies.

Audit information is to be considered confidential and shall not be disclosed to anyone for any purpose other than audit purposes or where required by law.

Information pertaining to a CA's management of a Subscriber's digital signature certificate shall only be disclosed to the Subscriber or where required by law.

SIGNATURE

The digital signature private key of each Subscriber is to be held only by the Subscriber and shall be kept confidential by them. Any disclosure of the private key or media containing the private key by the Subscriber is at the Subscriber's own risk.

CONFIDENTIAL

The Subscriber shall keep the Subscriber's copy of their confidentiality private key confidential. Disclosure by the Subscriber is at the Subscriber's own risk. Confidentiality keys may be backed up by the issuing CA in which case these keys shall be protected in accordance with Section 6, and shall not be disclosed without prior consent of the Subscriber or a duly authorized representative of the issuing CA unless required by law.

Any request for the disclosure of information shall be signed by the requestor and delivered in writing to the issuing CA. Any disclosure of information is subject to the requirements of any privacy laws and any other relevant legislation and applicable policy.

9.3.2 Information not within the scope of confidential information

Certificates, CRLs and personal or corporate information appearing in them and in public directories are not considered confidential information. Additionally, information that meets the following criteria shall not be considered to be confidential information:

55. Information that is documented by the receiving party as having been independently developed by it without unauthorized reference to or reliance on the confidential information of the disclosing party;
56. Information that the receiving party lawfully receives free of restriction from a source other than the disclosing party;
57. Information that is or becomes generally available to the public through no wrongful act or omission on the part of the receiving party;
58. Information that at the time of disclosure to the receiving party was known to the receiving party free of restriction as evidenced by documentation in the receiving party's possession; or
59. Information that the disclosing party agrees in writing is free of restrictions.

9.3.3 Responsibility to protect confidential information

A CA must ensure that confidential information be physically and/or logically protected from unauthorized viewing, modification or deletion. In addition, the CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

Confidentiality keys may be backed up by the issuing CA in which case these keys shall be protected in accordance with Section 6, and shall not be disclosed without prior consent of the Subscriber or a duly authorized representative of the issuing CA unless required by law.

9.4 Privacy of personal information

9.4.1 Privacy plan

Visa InfoDelivery PKI's policy is to not disclose private personal information of its Subscribers, customers, employees, and partners without the prior consent of the aforementioned unless required by law.

9.4.2 Information treated as private

Personal information, not appearing in certificates and in public directories, held by a CA or an RA (e.g. registration and revocation information, logged events, and correspondence between Subscriber and CA) is considered private and shall not be disclosed by the CA or RA.

9.4.3 Information not deemed private

Personal information that is publicly available, appearing in certificates and in public directories, is not considered private.

9.4.4 Responsibility to protect private information

A CA must ensure that private personal information be physically and/or logically protected from unauthorized viewing, modification or deletion. In addition, the CA must ensure that storage media used by the CA system is protected from environmental threats such as temperature, humidity and magnetism.

9.4.5 Notice and consent to use private information

Private personal information will only be utilized without prior consent as per section 9.4.1.

9.4.6 Disclosure pursuant to judicial or administrative process

Private personal information will only be disclosed if required by law as per section 9.4.1.

Any request for the disclosure of private information shall be signed by the requester and delivered in writing to the issuing CA. Any disclosure of private information is subject to the requirements of any privacy laws and any other relevant legislation and applicable organizational policy.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

The private key shall be the sole property of the legitimate holder of the corresponding public key identified in a certificate.

Each Visa PKI retains all intellectual property rights in and to the certificates and revocation information that it issued.

Visa Inc. retains all intellectual property rights in and to this CP.

9.6 Representations and warranties

A CA will issue and revoke or suspend certificates, operate its certification and repository services, and provide certificate status information in accordance with this CP.

Authentication and validation procedures will be implemented as set forth in Section 3 of this CP.

9.6.1 CA representations and warranties

All CAs shall operate in accordance with this CP, their respective CPS(s) and applicable laws, as described in Section 9.14, when issuing and managing certificates provided to subordinate CAs, RAs and Subscribers under this CP. CAs shall require that all the RAs operating on their behalf shall comply with the relevant provisions of this CP concerning the operations of the RAs. All CAs should provide notice of any limitation of liability (Section 9.8).

All CAs shall:

60. Issue and administer a CPS that is in compliance with this CP;
61. Issue certificates based on requests that are correctly and properly verified according to Section 3.1. A CA may delegate this verification (i.e., performing due diligence on the certificate requester and certificate request) to a registration authority (RA), but the CA retains responsibility for ensuring that these functions are performed properly.
62. Issue certificates only for use in conjunction with those applications that have been approved by the Visa Inc. Cryptographic Review Board as being appropriate to make use of this Visa InfoDelivery PKI.
63. Have in place mechanisms and procedures to make subordinate CAs, RAs, and Subscribers aware of and bound to the stipulations in this policy that apply to them;
64. Provide a secure environment and proper operations to protect the confidentiality and integrity of the CA; and
65. Through compliance audit, verify that the operation of the CA complies with this CP. If there are any material changes in the operation of the CA (e.g., change in location or CA configuration), the CA must notify the Visa Inc. Cryptographic Review Board immediately. If requested, the CA must and verify that the operation of the CA still is compliant with this CP through an audit.

When a CA publishes or delivers a certificate, it declares that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with this CP. Publication of the certificate in a repository, to which the Subscriber has access, or delivery of a signed certificate to a Subscriber, constitutes notice of such certification.

CA personnel associated with PKI roles shall be individually accountable for actions they perform. "Individually accountable" means that there shall be evidence that attributes an action to the person performing the action.

All issuing CAs shall take commercially reasonable measures to make Subscribers and Relying Parties aware of their rights and obligations with respect to the operation and management of any keys, certificates or hardware and software used in connection with the PKI. Subscribers should also be notified as to procedures for dealing with suspected key compromise, certificate or key renewal, and service cancellation.

9.6.2 RA representations and warranties

A CA shall require that all of its RAs, as defined in section 1.3.2, comply with all the relevant provisions of this CP, and the CA's CPS, in particular criteria for providing an RA service. The RAs must be contractually bound to comply with the Visa Inc By-laws, Operating Regulations and policies.

The RA is responsible for the identification and authentication of Subscribers following Sections 3.2 and 4.1. Subscriber's rights and obligations, as well as a description of a Relying Party's obligations with respect to use, verification and validation of certificates, will be communicated by the RA, on behalf of the CA, or provided by the Visa product or service participation agreement.

As delegated by the issuing CA, the RA may be responsible for revoking certificates in accordance with Section 4.9. The RA shall keep track of certificate expiration dates and request replacement certificates, in cooperation with the Subscriber, in a timely manner.

RAs shall be individually accountable for actions performed on behalf of a CA. Individually accountable means that there must be evidence that attributes an action to the person performing the action. Records of all actions carried out in performance of RA duties shall identify the individual who performed the particular duty. Each person performing RA duties shall protect his or her private keys, if applicable, in accordance with Section 4 and Section 6.

When an RA submits Subscriber information to a CA, it shall certify to that CA that it has authenticated the identity of that Subscriber and that the Subscriber is authorized to submit a certificate request in accordance with Section 3 and Section 4.

Submission of the certificate request, to the CA, is to be performed in a secure manner as described in section 3.2.

9.6.3 Subscriber representations and warranties

A CA shall require that a Subscriber has contractual agreements with Visa or a Visa Region or Client and are bound to comply with Visa Inc By-laws, Operating Regulations and policies and applicable Visa program or service agreements.

Any Subscriber information shall be complete, validated and accurate with full disclosure of all required information in connection with a certificate request.

The Subscriber shall only use its key pairs, and the associated certificates issued under this Visa InfoDelivery PKI, for the purposes identified in this CP. Key pairs intended for use in a production environment must be generated in that environment in accordance with the Visa security requirements that apply to the platform on which the keys reside. These key pairs must not be cloned, copied or otherwise conveyed for use in a test or development environment. Key pairs and the associated certificates shall not be shared by multiple functional entities. Key pairs generated in a non-production environment must not be used in production implementations of Visa products and services.

Subscribers are required to protect their private keys, associated passphrase(s) and tokens, as applicable, in accordance with Section 6, and to take all commercially reasonable measures to prevent their loss, disclosure, modification, or unauthorized use.

Where a Subscriber knows of or even suspects private key compromise, the Subscriber shall notify the issuing CA and/or RA in the manner specified by Section 4.9.

9.6.4 Relying party representations and warranties

Relying Parties must adhere to all Visa Inc By-Laws, Operating Regulations, policies, and applicable Visa program or service agreements that relate to specific instances in which a Relying Party trusts or otherwise makes use of a certificates issued within this Visa InfoDelivery PKI. In no event shall a Relying Party act in reliance upon a certificate that has expired or been revoked or suspended or that includes a revoked or suspended certificate in the chain of trust back to the Visa Root CA.

Prior to using a Subscriber's certificate, a Relying Party must verify that the certificate is appropriate for the intended use.

Prior to using a certificate, a Relying Party must check the status of the certificate using the appropriate certificate status publication method (e.g. CRL) in accordance with the requirements stated in Sections 4.4.10 and 4.4.11 or as otherwise prescribed by a relevant Visa Inc. policy or agreement. As part of this verification process the digital signature on the certificate status publication (e.g., CRL or OCSP message) must also be validated.

9.6.5 Representations and warranties of other participants

No Stipulation.

9.7 Disclaimers of warranties

This section is not meant to replace the liability and indemnifications provisions of the Visa Inc By-Laws, Operating Regulations and policies, which shall continue to be enforced and in effect.

Nothing in this CP shall confer on any third party any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of another except as set forth in this CP. Issuance of certificates in accordance with this policy does not make a CA or RA an agent, partner, joint venturer, fiduciary, trustee or other representative of Subscribers or

other Relying Parties. The applicable Subscriber Agreement or Relying Party Agreement defines the relationship between a CA, RA and the Subscriber.

9.8 Limitations of liability

In no event will the Visa InfoDelivery PKI be liable for any damages to Subscribers, Relying Parties or any other party arising out of or related to the misuse of, or reliance on Certificates issued by a CA that have been:

(i) Revoked or expired;
(ii) Used for unauthorized purposes;
(iii) Tampered with;
(iv) Compromised;
(v) Subject to misrepresentation, misleading acts or omissions.

Any disclaimer or limitations of liability will be consistent with this CP.

9.9 Indemnities

The indemnification obligations of Subscribers and Relying Parties shall be set forth in applicable Subscriber and Relying Part Agreements.

Unless otherwise set forth in this CP and/or Subscriber Agreement and/or Relying Party Agreement, Subscriber and/or Relying Party hereby agrees to indemnify and hold Visa InfoDelivery PKI harmless from any claims, actions or demands that are caused by the use or publication of a certificate and that arises from:

66. Any false or misleading statement of fact by the Subscriber;
67. Any failure by the Subscriber to disclose a material fact, if such omission was made negligently or with the intent to deceive;
68. Any failure on the part of the Subscriber to protect its Private Key and/or token if applicable, or to take the precautions necessary to prevent the compromise, disclosure, loss, modification or unauthorized use of the Subscriber's private key; or
69. Any failure on the part of the Subscriber to promptly notify a CA within the <ORGNAME> PKI of a compromise, disclosure, loss, modification or unauthorized use of the Subscriber's private key once actual or constructive notice of such event.

9.10 Term and termination

9.10.1 Term

This CP remains in force until notice of the opposite is communicated by Visa InfoDelivery CA on its web site at http://insite/primary/ref.cfm.

9.10.2 Termination

Termination of this document will be upon publication of a newer version or replacement document, or upon termination of CA operations.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this document will be communicated, on its web site at http://insite/primary/ref.cfm, upon termination outlining the provisions that may survive its termination and remain in force.

9.11 Individual notices and communications with participants

The Visa InfoDelivery PKI will define in any applicable agreement the appropriate provisions governing notices.

9.12 Amendments

Visa Inc. Cryptographic Review Board is the responsible authority for reviewing and approving changes to the Visa InfoDelivery PKI CP. Written and signed comments on proposed changes shall be directed to the Visa InfoDelivery PKI contact as described in Section 1.5. Decisions with respect to the proposed changes are at the sole discretion of the Visa Inc. Cryptographic Review Board.

9.12.1 Procedure for amendment

The Visa InfoDelivery PKI may provide notification, in writing, of any proposed changes to its Certificate Policy, if in the judgment and discretion of the Visa Inc. Cryptographic Review Board the changes may have significant impact on the issued certificates and Visa products or services. The notification will contain a statement of proposed changes, the final date of receipt of comments, and the proposed effective date of change. The Visa InfoDelivery CAs and participating CAs may notify their Subscribers of the proposed changes.

An electronic copy of the Visa PKI Disclosure Statement is to be made available at a web site at http://www.international.visa.com/fb/downloads/pki/main.jsp or by requesting an electronic copy by e-mail to the policy representative as described in Section 1.5.

Written and signed comments on proposed changes shall be directed to the Visa Inc. Cryptographic Review Board as described in Section 1.5. Decisions with respect to the proposed changes are at the sole discretion of the Visa Inc. Cryptographic Review Board.

The period of time that affected parties have to conform to the change will be defined in the notification.

9.12.2 Notification mechanism and period

The Visa Inc. Cryptographic Review Board will post the change notification, if necessary, at the CP publishing point (http://insite/global/CorpKeyControls/information/DigitalCertificates.aspx).

If a policy change is determined by the Visa Inc. Cryptographic Review Board to warrant the issuance of a new policy, the Visa Inc. Cryptographic Review Board will assign a new Object Identifier (OID) for the new policy.

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

9.12.3 Circumstances under which OID must be changed

If a policy change is determined by the Visa InfoDelivery PKI to warrant the issuance of a new policy, the Visa InfoDelivery PKI will assign a new Object Identifier (OID) for the new policy.

9.13 Dispute resolution provisions

Refer to Visa Inc. Operating Regulations.

9.14 Governing law

Refer to Visa Inc. Operating Regulations.

9.15 Compliance with applicable law

Refer to Visa Inc. Operating Regulations.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Refer to Visa Inc. Operating Regulations.

9.16.2 Assignment

Refer to Visa Inc. Operating Regulations.

9.16.3 Severability

Refer to Visa Inc. Operating Regulations.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

Refer to Visa Inc. Operating Regulations.

9.16.5 Force Majeure

The Visa InfoDelivery PKI shall not be held responsible for any delay or failure in performance of its obligations hereunder to the extent such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, acts of terrorism or war, act of God, or other similar causes beyond its reasonable control and without the fault or negligence of the delayed or non-performing party or its subcontractors.

9.17 Other provisions

No stipulation

ABBREVIATIONS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
OCSP	On-line Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest-Shamir-Adleman
SHA –1	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

GLOSSARY

A

TERM: Access control
DEFINITION: The granting or denial of use or entry. Specifically, allowing or denying access to some component of the PKI such as key component, CA system or CA facility.

TERM: Activation Data
DEFINITION: Data (other than the keys themselves) that are used and needed to activate a private key. Examples include: PIN, password, or portion of a key or other data used to enforce multi-person control over a private key.

TERM: Administrator
DEFINITION: A Trusted Person within the organization of a Region, Client or their designated agent (i.e., third party certificate service provider) that performs validation and other CA or RA functions.

TERM: Administrator Certificate
DEFINITION: A Certificate issued to an Administrator that may only be used to perform CA or RA functions.

TERM: Authentication
DEFINITION: The act of verifying. In the case of identities, this would be establishing the assurance of an identity.

TERM: Authorization
DEFINITION: The granting of permissions of use.

TERM: ANSI X9.30
DEFINITION: United States financial industry standard for digital signatures based on the federal Digital Signature Algorithm (DSA). ANSI X9.30 requires the SHA1 hash algorithm

B

TERM: Business process
DEFINITION: A set of one or more linked procedures or activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships.

C

TERM: Certificate
DEFINITION: The public key of a user, together with related information, digitally signed with the private key of the Certification Authority that issued it. The certificate format is in accordance with ITU-T Recommendation X.509. Certificates are typically used to verify the identity of an individual, organization, device or application. They are also used to ensure message integrity through private key signature and enable confidentiality of data through public key encryption.

TERM: Certificate Chain
DEFINITION: An ordered list of Certificates containing an end entity Subscriber Certificate, the CA certificate that signed it, and all of the CA Certificates up to the root certificate forming a 'chain' of certificates from end entity to root CA.

TERM: Certification Authority

DEFINITION: An authority trusted by one or more users to issue and manage X.509 certificates and CRLs. Certification Authorities have certificates that allow them to sign other certificates and/or certificate revocation lists (CRLs). Within the Visa InfoDelivery PKI, Certification Authority Subscribers include:

- Visa InfoDelivery Root and Brand CAs that may issue certificates to subordinate Certificate Authorities and / or end entities within the Visa InfoDelivery PKI
- Participating CAs (subordinate to Visa Brand CAs) that may only issue end entity certificates.

TERM: Certificate Policy (CP)
DEFINITION: Named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. It is the principal statement of certificate policy governing the Visa InfoDelivery PKI. The CP is a high-level document that describes the requirements, terms and conditions, and policy for issuing, utilizing and managing certificates issued by a CA.

TERM: Certification Practice Statement (CPS)
DEFINITION: A statement of the practices that a Certification Authority employs in issuing certificates. It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management and will be more detailed than the certificate policies supported by the CA. The CPS must illustrate how the CA satisfies the requirements included in the CP that governs it.

TERM: Certificate Revocation List
DEFINITION: A periodically issued list, digitally signed by the issuing CA, of certificates issued by that CA that have been revoked or suspended prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked certificates' serial numbers, and the specific times and reasons for revocation. CRLs are used to check the status of certificates; they may be published on a repository or an OCSP responder.

TERM: Confidential
DEFINITION: A security classification used to describe information which if disclosed could result in personal loss or minor financial loss. Personal information and tactical information would be deemed confidential.

TERM: Confidentiality
DEFINITION: Information that has an identifiable value associated with it such that if disclosed might cause damage to an entity.

TERM: Cross Certification
DEFINITION: The process describing the establishing of trust between two or more CAs. It usually involves the exchange and signing of CA certificates between two CAs in different PKI hierarchies and involves the verification of assurance levels.

D
TERM: Digital Signature
DEFINITION: The result of the transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine that the key that corresponds to the signer's key created the transformation and the message was not altered.

TERM: Distinguished Name (DN)
DEFINITION: A DN is used in a certificate to uniquely identify a certificate-owner (Subscriber) or a certificate issuer (Certification Authority). The Issuer and Subject Distinguished Names in a

certificate are formed from a combination of the following possible attributes (also referred to as relative distinguished names):

- Common Name (cn)
- Country (c)
- Organization name (on)
- Organizational unit name (ou)
- Locality (l)
- State or Province (st)
- User id
- Domain component (dc)
-

No two certificates issued by a particular CA can have the same DN.. Examples of DNs include:

cn=Road Runner, ou=bird, on=mammal, c=US
ou=bird, dc=carton, dc=com

Every entry in an X.500 or LDAP directory has a Distinguished Name. It is a unique entry identifier throughout the complete directory. No two entries within the same directory can have the same DN.

TERM: Dual Control
DEFINITION: A process utilizing two or more separate entities (usually persons), operating in concert, to protect sensitive functions or information, whereby no single entity is able to access or utilize the materials, e.g., cryptographic key.

E
TERM: E-mail Certificates
DEFINITION: Certificates utilized for encrypting and verifying digital signatures. Normally two separate certificates: one for encryption, the other for signature verification.

TERM: End Entity Subscriber
DEFINITION: End entity Subscribers have certificates that can only be used for authentication, confidentiality or message integrity. End entity Subscribers cannot themselves issue certificates (i.e., they are not CAs). End entity Subscribers include:

- Individuals associated directly with or through the agents of the Visa Brand, a Region or a Member Client (i.e., cardholders, merchants and employees).
- Organizations (e.g., Visa Regions, Clients or their agents, merchants)
- Devices or applications (e.g., servers, client software) to be used by the Visa Brand, Region Client or its agent in conjunction with the delivery of a Visa product or service.
- Visa personnel issued certificates for the purpose of administering a CA.

TERM: Entity
DEFINITION: Any autonomous element or component within the Public Key Infrastructure that participates in one form or another, such as managing certificates or utilizing certificates. An Entity can be a CA, RA, Subscriber, Relying Party, etc.

F
TERM: FIPS 140-2
DEFINITION: Federal Information Processing Standard 140-2 (FIPS 140-2) is a standard that describes US Federal government requirements that IT products should meet for Sensitive, but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian government's Communication Security Establishment (CSE), and may be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard provide different levels of security and in the higher levels, have different documentation requirements.

TERM: FIPS 180-1
DEFINITION: Standard specifying the Secure Hash Algorithm, SHA-1, for computing a condensed representation of a message or a data file.

G
H
I
TERM: Integrity
DEFINITION: ensuring consistency of an object or information. Within security systems, integrity is the principle of ensuring that a piece of data has not been modified maliciously or accidentally.

J
K
TERM: Key
DEFINITION: When used in the context of cryptography, it is a value (which may be secret), a sequence of characters that is used to encrypt and decrypt data. A key is a unique, generated electronic string of bits used for encrypting, decrypting, creating digital signatures or validating digital signatures.

TERM: Key Pair
DEFINITION: Often referred to as a public/private key pair. One key is used for encrypting (or digitally signing) and the other key used for decrypting (or signature validation). Although related, the keys are sufficiently different that knowing one does not allow derivation or computation of the other. This means that one key can be made publicly available without reducing security, provided the other key remains private.

L
M
TERM: MD5
DEFINITION: One of the message digest algorithms developed by RSA Security Inc.

N
TERM: non-repudiation
DEFINITION: protection against the denial of the transaction or service or activity occurrence.

O
TERM: OCSP (Online Certificate Status Protocol)
DEFINITION: An online protocol developed by the IETF (RFC 2560) to allow a Relying Party to obtain more timely information regarding the revocation status of a certificate than is possible with CRLs.

TERM: Object Identifier
DEFINITION: The unique alphanumeric identifier registered under the ISO registration standard to reference a standard object or class.

P
TERM: Participating CA
DEFINITION: Within the Visa InfoDelivery PKI hierarchal model, Visa Regions and Clients may become CAs subordinate to the Visa Brand CAs. These CAs are referred to as “participating CAs”.

TERM: PKCS #1

DEFINITION: Standard that provides recommendations for the implementation of public-key cryptography based on the RSA algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes, etc.

TERM: PKCS #7
DEFINITION: A cryptographic message format or syntax managed and edited by RSA Laboratories. A standard describing the general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes. This format is frequently used by CAs to transmit a certificate to the requesting Subscriber.

TERM: PKCS #10
DEFINITION: A certificate request format or syntax managed and edited by RSA Laboratories. It is a standard describing syntax for a request for certification of a public key, a name, and possibly a set of attributes.

TERM: PKIX
DEFINITION: The Public Key Infrastructure (X.509) or PKIX is an IETF Working Group established with the intent of developing Internet standards needed to support an X.509-based PKI. The scope of PKIX extends to also develop new standards for use of X.509-based PKIs in the Internet.

TERM: PKI personnel
DEFINITION: Persons, generally employees, associated with the operation, administration and management of a CA or RA.

TERM: Policy
DEFINITION: The set of laws, rules and practices that regulates how an organization manages its business. Specifically, security policy would be the set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive information.

TERM: PrintableString
DEFINITION: String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself. PrintableString characters include: A-Z, a-z, 0-9, space ‘ ( ) + , - . / : = ?

TERM: Private Key
DEFINITION: The private key is one of the keys in a public/private key pair. This is the key that is kept secret as opposed to the other key that is publicly available. Private keys are utilized for digitally signing documents, uniquely authenticating an individual, or decrypting data that was encrypted with the corresponding public key.

TERM: Public Key Infrastructure
DEFINITION: A set of policies, procedures, technology, audit and control mechanisms used for the purpose of managing certificates and keys.

TERM: Public
DEFINITION: A security classification for information that if disclosed would not result in any personal damage or financial loss.

TERM: Public Key
DEFINITION: The community verification key for digital signature and the community encryption key for encrypting information to a specific end entity.

Q
R

TERM: Registration Authority
DEFINITION: An entity that performs registration services on behalf of a CA. RAs work with a particular CA to vet requests for certificates that will then be issued by the CA.

TERM: Rekey
DEFINITION: the process of replacing the key(s). The expiration of the crypto period involves the replacement of the public key in the certificate and therefore the generation of a new key pair and associated certificate request.

TERM: Relative Distinguished Name (RDN
DEFINITION: A Distinguished Name is made up of a sequence of Relative Distinguished Names, or RDNs. The sequences of RDNs are separated by commas (,) or semi-colons (;). There can be more than one identical RDN in a directory, but they must be in different bases, or branches, of the directory. Example of a DN is "cn=Road Runner, ou=bird, on=mammal, c=US".

RDNs would be:
RDN => cn=Road Runner
RDN => ou=bird
RDN => on=mammal
RDN => c=US

TERM: Relying Party
DEFINITION: A person or entity that is authorized to act in reliance upon a certificate issued within the Visa PKI (including by means of devices under their control). Relying Parties within the Visa PKI **must** have a valid business relationship with Visa and be contractually bound to comply with the Visa Inc By-Laws, Operating Regulations and policies. [Note possibility of requiring adherence to a relevant relying party agreement.]

TERM: Relying Party Agreement
DEFINITION: A relying party agreement is entered into by a party wishing to rely on a certificate and the information contained in it. A relying party agreement governs the terms and conditions under which the relying party is permitted to rely upon the certificate. Most commonly, the agreement requires the relying party to check the status of the certificates in the chain of certificates upon which the relying party wishes to rely. For Visa products and services, relying party agreements are typically contained within the applicable Visa product or service participation agreement.

TERM: Repository
DEFINITION: A place or container where objects are stored. A data repository is technology where data is stored logically. In PKI terms, a repository accepts certificates and CRLs from one or more CAs and makes them available to entities that need them for implementing security services.

TERM: Revocation
DEFINITION: In PKI, revocation is the action associated with revoking a certificate. Revoking a certificate is to make the certificate permanently invalid before its normal expiration. The Certification Authority that issued the certificate is the entity that revokes a certificate. The revoked status is normally published on a certificate revocation list (CRL) and/or posted on an OCSP responder.

TERM: RSA
DEFINITION: A public key cryptographic algorithm invented by Rivest, Shamir, and Adelman..

S
TERM: Secret

DEFINITION: A security classification used to describe the most sensitive information which if disclosed could result in severe and adverse impact to the company or its employees. Visa includes keys and keying material, PINs and passwords as secret information.

TERM: Sensitive
DEFINITION: Used to describe the security classification of information where the information if disclosed would result in serious financial loss, serious loss in confidence or could result in personal harm or death. Visa defines sensitive information as including information classified as either Visa secret or Visa confidential.

TERM: Signature Verification Certificate
DEFINITION: Often referred to as simply a Signature Certificate. It is the certificate containing the public key used to verify a digital signature that was signed by the corresponding private key.

TERM: Split Knowledge
DEFINITION: a condition under which two or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key. The resultant key exists only within secure cryptographic devices

TERM: SSL Client Certificate
DEFINITION: Certificate utilized to verify the authentication of an end entity to a server when a connection is being established via a SSL session (secure channel).

TERM: SSL Server Certificate
DEFINITION: Certificate utilized to verify the authentication of a web or application server to the end entity (client) when a connection is being established via a SSL session (secure channel).

TERM: Subscriber
DEFINITION: A Subscriber is an entity; a person, device or application that is a holder of a private key corresponding to a public key, and has been issued a certificate. In the case of a device, a person authorized by the organization owning the device may be referred to as the Subscriber. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the certificate. There are two categories of Subscribers: end entities and certification authorities.

TERM: Subscriber Agreement
DEFINITION: A Subscriber agreement is an agreement entered into by a subscriber obtaining a certificate that will contain the terms and conditions of the use of the subscriber's certificate and private key corresponding to the public key contained in the certificate. For Visa products and services, subscriber agreements are typically contained within the applicable Visa product or service participation agreement.

TERM: Suspension
DEFINITION: In PKI, suspension is the action associated with suspending a certificate. Suspending a certificate is to make the certificate invalid for a period of time while a condition that might result in revocation is investigated. During the suspension period, the suspended certificate will be listed on the issuing CA's CRLs as 'on hold' and treated by Relying Parties as revoked. At the end of the suspension period, the certificate will be re-instated or revoked. The Certification Authority that issued the certificate is the entity that suspends a certificate. The suspended status is normally published on a certificate revocation list (CRL) and / or posted on an OCSP responder. Suspending a certificate can potentially avoid an unnecessary or unwarranted revocation.

T
TERM: Threat

DEFINITION: a danger to an asset in terms of that asset's confidentiality, integrity, availability or legitimate use.

U

TERM: URI

DEFINITION: Uniform Resource Indicator - an address on the Internet. The most common version of URI is the URL (Uniform Resource Locator).

TERM: UTF8String

DEFINITION: UTF-8 is a type of Unicode, which is a character set supported across many commonly used software applications and operating systems. UTF-8 is a multi-byte encoding in which each character can be encoded in as little as one byte and as many as four bytes. Most Western European languages require less than two bytes per character. Greek, Arabic, Hebrew, and Russian require an average of 1.7 bytes. Japanese, Korean, and Chinese typically require three bytes per character. Such Unicode is important to ensure universal characters/foreign characters are supported. After December 31, 2003, all certificates must use UTF8String encoding for subject names.

V

TERM: Vettor

DEFINITION: A person who verifies information provided by a person applying for a certificate.

TERM: Visa Inc CA

DEFINITION: This is comprised of the Visa Root CA and the Visa Brand CAs (subordinate to the Visa Root CA) that are at the top of the Visa PKI. The Visa Root CA is an offline CA that only issues certificates to Visa Brand CAs. The Visa Brand CAs may be either offline or online and issue certificates to the following Subscribers:

- End entities (i.e., individuals associated directly with or through the agents of the Visa Regions, Clients or their agents)
- Certification Authorities (Regions or Clients only)

TERM: Visa International Public Key Infrastructure (PKI) or Visa PKI

DEFINITION: This is an X.509 PKI implemented by Visa for issuing and managing digital certificates to be used in conjunction with Visa products and services. This PKI consists of a hierarchy of entities called certification authorities (CAs) that issue certificates to Subscribers (i.e., end entities or other CAs) within the hierarchy. The term Visa PKI is used to refer to all of the Subscribers from the Visa International Root CA all the way down to the lowest level end entity.

TERM: Visa Products and Services

Visa programs that are associated with the Visa-Owned Mark. These include both the products (e.g., Visa Gold Card) and the underlying services operated by Visa or its agents (e.g., VisaNet, VbV Directory) that are used to support these products.

TERM: Vulnerability

DEFINITION: weaknesses in a safeguard or the absence of a safeguard.

W

X

TERM: X.500

DEFINITION: Specification of the directory service required to support X.400 e-mail initially but common used by other applications as well.

TERM: X.501 PrintableString

DEFINITION: String format for representing names, such as Common Name (CN), in X.509 certificates. The encoding of a value in this syntax is the string value itself; an arbitrary string of printable characters. The characters included in this set include:

A,B,…,Z
a,b,…,z
0,1,…,9
(space) ‘ ( ) + , - . / : = ?

TERM: X.509
DEFINITION: An ISO standard that describes the basic format for digital certificates.

Y
Z