

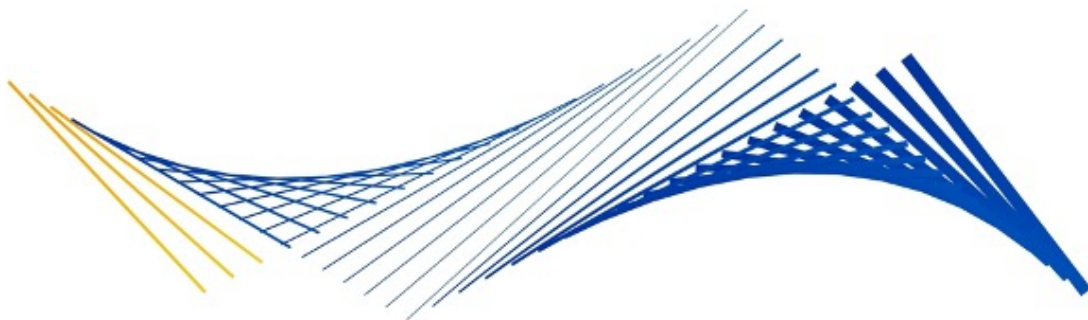


Visa Public Key Infrastructure Certificate Policy (CP) for Internal Trust

Version 1.2

Visa PKI

March 16, 2026



Contents

Important Note on Confidentiality and Copyright	3
About This Guide	4
Audience	4
1. INTRODUCTION	5
1.1. Overview	5
1.2. Document Name and Identification	7
1.3. PKI Participants	8
1.4. Certificate Usage	9
1.5. Policy Administration	9
1.6. Definitions and Acronyms	10
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	17
2.1. Repositories	17
2.2. Publication of Information	17
2.3. Time or Frequency of Publication	17
2.4. Access Controls on Repositories	17
3. IDENTIFICATION AND AUTHENTICATION	18
3.1. Naming	18
3.2. Initial Identity Validation	19
3.3. Identification and Authentication for Re-Key Requests	21
3.4. Identification and Authentication for Revocation Requests	22
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	23
4.1. Certificate Application	23
4.2. Certificate Application Processing	23
4.3. Certificate Issuance	24
4.4. Certificate Acceptance	24
4.5. Key Pair and Certificate Usage	24
4.6. Certificate Renewal	25
4.7. Certificate Re-Key	25
4.8. Certificate Modification	25
4.9. Certificate Revocation and Suspension	26
4.10. Certificate Status Services	28
4.11. End of Subscription	29
4.12. Key Escrow and Recovery	29
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS	30
5.1. Physical Security Controls	30
5.2. Procedural Controls	31
5.3. Personnel Controls	32
5.4. Audit Logging Procedures	33
5.5. Records Archival	35

5.6. Key Changeover	35
5.7. Compromise and Disaster Recovery	35
5.8. CA or RA Termination	36
6. TECHNICAL SECURITY CONTROLS	37
6.1. Key Pair Generation and Installation	37
6.2. Private Key Protection and Cryptographic Module Engineering Controls	38
6.3. Other Aspects of Key Pair Management	39
6.4. Activation Data	39
6.5. Computer Security Controls	39
6.6. Life Cycle Technical Controls	40
6.7. Network Security Controls	40
6.8. Time-Stamping	40
7. CERTIFICATE, CRL, AND OCSP PROFILES	41
7.1. Certificate Profile	41
7.2. CRL Profile	43
7.3. OCSP Profile	43
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	45
8.1. Frequency or Circumstances of Assessment	45
8.2. Identity and Qualifications of Assessor	45
8.3. Assessor's Relationship to Assessed Entity	45
8.4. Topics Covered by Assessment	45
8.5. Actions Taken as a Result of Deficiency	45
8.6. Communication of Results	45
8.7. Self-Audits	46
9. OTHER BUSINESS AND LEGAL MATTERS	47
9.1. Fees	47
9.2. Financial Responsibilities	47
9.3. Confidentiality of Business Information	47
9.4. Privacy of Personal Information	48
9.5. Intellectual Property Rights	49
9.6. Representations and Warranties	49
9.7. Disclaimers of Warranties	52
9.8. Limitations of Liability	52
9.9. Indemnities	52
9.10. Term and Termination	53
9.11. Individual Notices and Communications with Participants	53
9.12. Amendments	53
9.13. Dispute Resolution Provisions	53
9.14. Governing Law	53
9.15. Compliance with Applicable Law	54
9.16. Miscellaneous Provisions	54
9.17. Other Provisions	54

Important Note on Confidentiality and Copyright

This document is protected by copyright restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Visa.

Visa and other trademarks are trademarks or registered trademarks of Visa.

All other product names mentioned herein are the trademarks of their respective owners.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE PUBLICATION. VISA MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS PUBLICATION AT ANY TIME.

If you have technical questions or questions regarding a Visa service or questions about this document, please contact your Visa representative.

About This Guide

Visa Certificate Policy (CP) for Internal Trust is the first in a set of documents related to the *Internal Visa Public Key Infrastructure (PKI)* operations.

Audience

The target audience for this document includes Visa entities such as Business Groups, Visa subsidiaries, and Visa clients and their agents who use Visa-issued certificates in conjunction with Visa products and/or services.

1. INTRODUCTION

1.1. Overview

A Public Key Infrastructure (PKI) system is an umbrella term for a collection of Certificate Authorities (CAs), computer applications, people, and processes that issue digital certificates.

A CA with functions that are performed by the PKI administrators issues CA certificates to the Issuing CA as well as End-Entity certificates.

The Visa Certificate Policy (CP) describes the business and technical requirements and provides the framework and context within which certificates are requested, created, issued, renewed, managed, revoked and/or used by participants of the Visa PKIs.

The Visa PKIs issue certificates for use in conjunction with various Visa products and 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 of transactions.

Visa PKI certificates must only be used in conjunction with Visa products and services unless Visa grants prior approval by the Visa Cryptographic Review Forum (CRF).

With the exception of the Visa Smart Debit/Credit (VSDC) PKI, CA certificates can only be issued to Visa or Visa Business Groups. For the VSDC PKI only, Visa clients may be issued CA certificates known as Issuer Public Key (IPK) certificates in VSDC.

CA certificates may be renewed.

End-Entity certificates are used for authentication, data integrity, and confidentiality but they must not be used to sign CA certificates or Certificate Revocation Lists (CRLs). These End-Entity certificates can be issued to Visa business groups, Visa clients and their agents, employees, merchants, and cardholders. Root CAs must not issue End-Entity certificates. End-Entity certificates cannot be renewed.

Reliance upon Visa PKI issued certificates is limited to entities that have agreed to the Visa By-Laws, Operating Regulations, policies, or operative commercial agreement. No other person or entity may rely upon Visa PKI issued certificates for any other purpose.

The type of certificates issued will vary depending upon the product and service.

The certificate request process may vary by product or service. Certificate requests may be processed either electronically or manually.

At the top of the Visa PKI hierarchy are the following Root CAs:

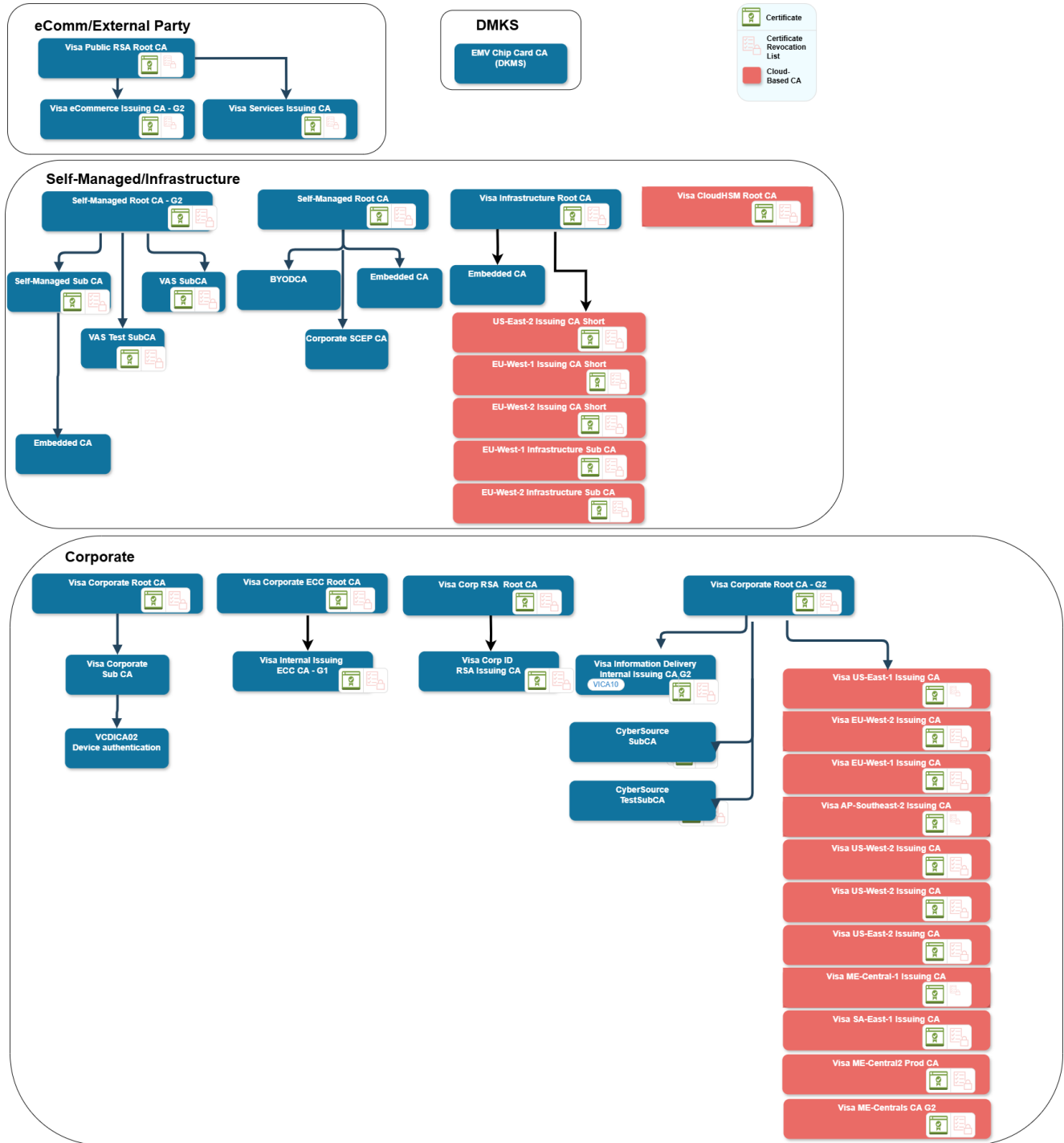
- Visa Public RSA Root CA
- Visa Corporate Root CA
- Visa Corporate Root CA G2
- Visa Corp RSA Root CA
- Visa Self Managed Root CA
- Visa Self Managed Root CA G2
- Visa Infrastructure Root CA
- Visa Corporate ECC Root CA
- Visa CloudHSM Root CA

The CAs are organized in hierarchies as follows:

1. **Root CAs** are at the top of the hierarchy.
2. **Intermediate Issuing CAs** are directly subordinate to the Root CAs, which have subordinate Issuing CAs.
3. **Issuing CAs** are the lowest level of the hierarchy, and only issue End-Entity certificates. They are subordinate to the Intermediate CAs or Root CAs.

The following figure illustrates the Visa PKI hierarchies.

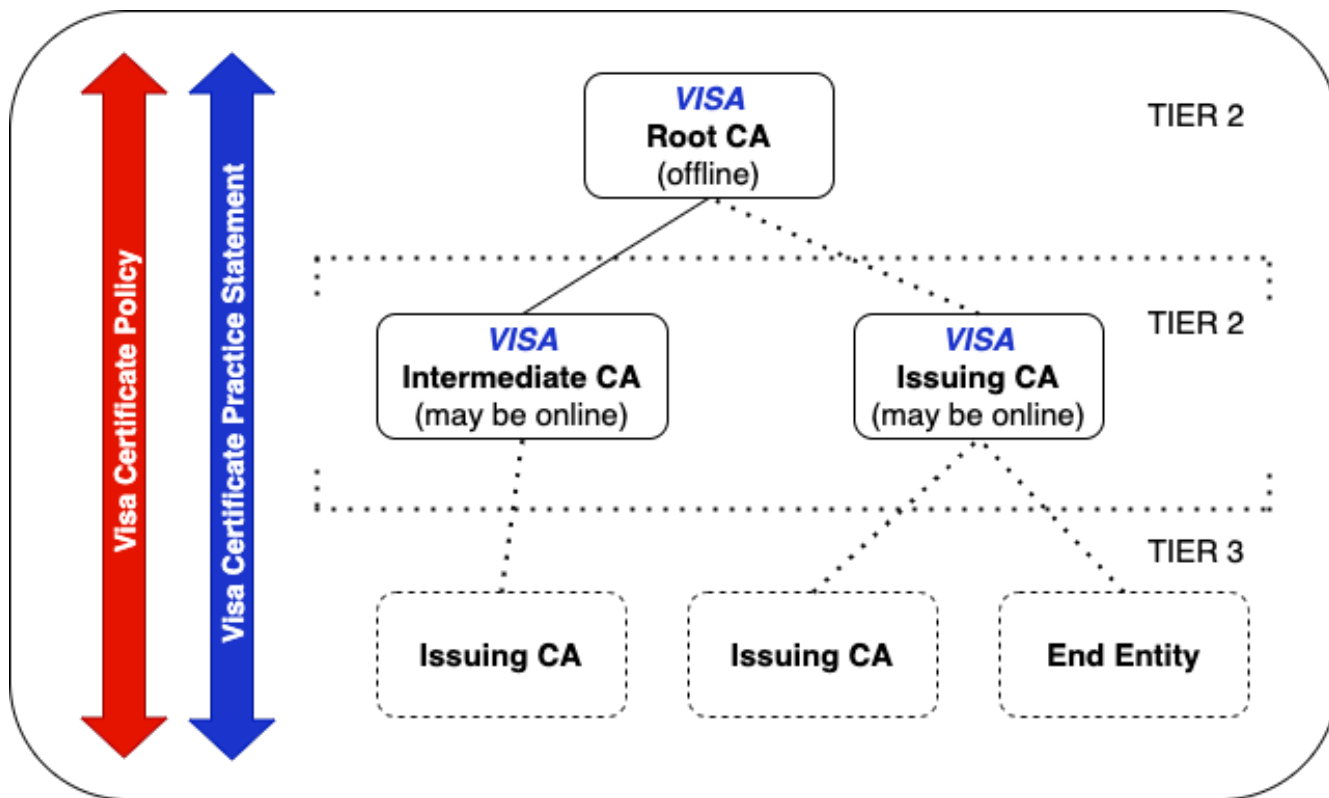
Figure 1–1: Visa PKI Hierarchies



Cross-certification between external CAs and CAs is not supported. The Visa PKI hierarchy is a closed PKI. As shown in the following figure, the Visa CPS applies to Visa CAs. Other documents, such as general security

policies, operation procedures, key ceremony guides, disaster recovery plans, and so on, may also supplement this Visa CP and the Visa CPS.

Figure 1–2: Visa Document Structure



This Visa CP generally conforms to the Internet Engineering Task Force (IETF) Public Key Infrastructure Extensions (PKIXs) Internet X.509 PKI Certificate Policy and Certification Practice Statement Framework (also known as RFC 3647).

Visa has implemented multiple X.509 PKIs and EMVCo PKI for issuing and distributing digital certificates in support of Visa products and services. This infrastructure is known as the Visa PKIs and is made up of a hierarchy of entities called CAs.

A CA is a trusted third-party that issues digital certificates to Subscribers (End-Entities or other CAs) within the hierarchy.

1.2. Document Name and Identification

The Object Identifiers (OIDs) used for certificates issued under this CP are:

- OID: 2.23.131.1.1 – Visa eCommerce PKI
- OID: 2.23.131.2.1 – Visa Information Delivery PKI
- OID: 2.23.131.3.1 - Visa Corporate PKI

1.2.1. Revisions

Version	Details	Date
1.0	Initial Draft.	30 November 2025
1.1	Remove Visa Public ECC Root CA from Internal CAs	24 February 2026
1.2	Updated to clarify the scope of applicability by explicitly including operative commercial agreements	16 March 2026

1.2.2. Relevant Dates

1.3. PKI Participants

The Visa CP governs the Visa PKIs and Subscribers that are issued certifications by a CA. Visa does not have delegated third-parties.

1.3.1. Certification Authorities

Certificate Authorities' functions are performed by PKI administrators. CAs sign public certificates that bind Subscribers to their private keys operating within the Visa PKIs and are responsible for:

- Creating and signing certificates binding Subscribers CAs. For more information, refer to "Subscribers".
- Publishing certificate status through CRLs or Online Certificate Status Protocol (OCSP), if supported by Relying Parties. For more information, refer to "Relying Parties".
- Requiring adherence to the Visa CP.
- Creating, storing, and recovering End-Entity confidential key pairs, if required.

A CA may have other duties delegated by the CRF. A CA PKI administrator may perform duties on more than one CA. A CA PKI administrator must be an employee of Visa.

1.3.2. Registration Authorities

Registration Authorities' (RAs) functions are performed by Vectors and are approved by a CA.

RAs are responsible for:

- Establishing enrollment procedures and processing certificate requests.
- Ensuring that certificate request has been transferred to/from the originator in a secured manner.
- Identification and authentication of certificate applicants.
- Verifying that the party submitting the certificate request is:
 - Who they claim to be
 - Is authorized to submit the request on behalf of the certificate request originator
 - Has a valid business relationship with Visa consistent with the certificate request
- Initiating or passing along revocation or certificate status change requests.
- Verifying that certificate revocation requests are from people whose identity is verified and that they are authorized to submit the revocation request.
- Approving applications for issue, revocation, or reissue of certificates.

An RA may have other duties delegated by the CA or the CRF. An RA may perform duties on more than one CA. RA staff must be a Visa employee or contractor.

1.3.3. Subscribers

A Subscriber is a person, device or application that is issued a digital certificate.

The certificate binds a public/private key pair to a single Subscriber. For a device or application, the person authorized by the organization may also be referred to as the Subscriber. Subscribers must have a valid business relationship and must be contractually bound to comply with the Visa By-Laws, Operating Regulations, policies, or operative commercial agreement.

There are two categories of Subscribers:

End-Entity Subscribers are individuals or organizations that obtain certificates for use with Visa products and services. End-Entity Subscribers have certificates that must only be used for authentication, confidentiality, or message integrity. An End-Entity Subscriber's eligibility is at the discretion of the Issuing CA and should be consistent with Visa's overall policies. End-Entity Subscribers include:

- Individuals (that is, employees or contractors of Visa, Visa clients or their agents)
- Devices or applications (for example, servers or client software) used

CA Subscribers may sign other certificates or CRLs and may administer any number of CA Subscribers. These Subscriber's certificates may be used for authentication, confidentiality, or message integrity. CA Subscribers include:

- Intermediate CAs who must only issue and sign certificates to Issuing CAs
- Issuing CAs who must only issue and sign End-Entity certificates

1.3.4. Relying Parties

Relying Parties (RPs) are persons or entities that trust a digital certificate. RPs must have a valid business relationship and be contractually bound to comply with the Visa By-Laws, Operating Regulations, policies, or operative commercial agreement.

1.3.5. Other Participants

No stipulations.

1.4. Certificate Usage

Certificate usage implies the certificate's full life-cycle, including the issuance, usage, suspension, revocation, and expiration of digital certificates.

1.4.1. Appropriate Certificate Uses

Digital certificates may be used for integrity and authenticity of business transactions and used for encryption of information.

1.4.2. Prohibited Certificate Uses

Other uses of digital certificates, unless specified in "Appropriate Certificate Uses", are prohibited.

1.5. Policy Administration

Visa CRF is the administrative authority of the Visa CP.

1.5.1. Organization Administering the Document

The Visa CRF is the authority for reviewing and approving changes to this Visa CP. Proposed changes or comments must be directed to the CRF contact as shown below. Decisions to proposed changes are at the sole discretion of the CRF.

1.5.2. Contact Person

Chairman, Visa Cryptographic Review Forum
Mailstop: M2-10910
800 Metro Center Blvd
Foster City, CA 94404-2775
PKIPolicy@visa.com

1.5.3. Person Determining CPS Suitability for the Policy

Visa CRF approves the Visa CPS which is subordinate to the Visa CP.

1.5.4. CPS Approval Procedures

The Visa CRF reviews any modifications, additions, or deletions to the Visa's CP/CPS and determines if these changes are acceptable. At its sole discretion, the Visa CRF must approve or reject any proposed changes to the Visa CPS.

1.6. Definitions and Acronyms

1.6.1. Definitions

Access control: 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.

Activation Data: Data (other than the keys themselves) that are used and needed to activate a private key. For example, Personal Identification Number (PIN), password, or a portion of a key or other data used to enforce multi-person control over a private key.

Administrator: A trusted person within the organization of a region, client, or their designated agent (that is, third-party certificate service provider) that performs validation and other CA or Registration Authority (RA) functions.

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

Authentication: The act of verifying identities. In the CAs, this would be validating an identity.

Authorization: The granting of permissions of use.

ANSI X9.30: U.S. financial industry standard for digital signatures based on the federal Digital Signature Algorithm (DSA). American National Standards Institute (ANSI) X9.30 requires the SHA1 hash algorithm.

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

Certificate: The public key of a user, together with related information, digitally signed with the private key of the CA that issued the certificate. The certificate format is in accordance with International Telecommunication Union (ITU)-T Recommendation X.509 or other Visa-accepted standard such as EMVCo. Typically, certificates are used to verify the identity of an individual, organization, device, or an application. They are also used to ensure message integrity through private key signature and enable confidentiality of data through public-key encryption.

Certificate Chain: 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 CA.

Certificate Authority: An authority trusted by one or more users to issue and manage X.509 certificates and Certificate Revocation Lists (CRLs). The CAs have certificates that allow them to sign other certificates and/or CRLs. Within the Visa PKI, CA Subscribers include:

- Root and Issuing CAs that may issue certificates to subordinate CAs and/or End-Entities within the PKI.
- Issuing CAs that may only issue End-Entity certificates.

Certificate Policy (CP): A 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 PKI. The Visa CP is a high-level document that describes the requirements, terms and conditions, and policy for issuing, using, and managing certificates issued by a CA.

Certification Practice Statement (CPS): A statement of the practices that a CA uses 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. It is more detailed than the certificate policies supported by the CA. The CPS illustrates how the CA satisfies the requirements included in the CP that governs it.

Certificate Revocation List (CRL): 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 might be published on a repository or through an Online Certificate Status Protocol (OCSP) responder.

Certificate Systems: The system used by a CA or Delegated Third-Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Confidential: Information that has an identifiable value associated with it such that if disclosed, might cause damage to an entity.

Cross-Certification: The process describing the establishment 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.

Delegated Third Party: A natural person or legal entity that is not the Visa CA and that operates any part of a Certificate System.

Digital Signature: 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 that the message was not altered.

Distinguished Name: A Distinguished Name (DN) is used in a certificate to identify a certificate owner (Subscriber) or a certificate issuer (Certificate Authority). The Issuer and Subject DNs in a certificate are formed from a combination of the following possible attributes (also referred to as relative DNs):

- Common Name(cn)
- Country(c)
- Organization name(on)
- Organizational unit name(ou)
- Locality(l)
- State or Province(st)
- Email Address(e)
- UserID
- Domain component(dc)

Domain Contact: The Domain Name Registrant, technical contact, administrative contact, or equivalent contact as identified through Domain Control Validation (DCV) methods, a DNS SOA record, or through direct contact with the Domain Name Registrar. References to WHOIS records, including those under ccTLDs, are excluded due to the sunset of WHOIS usage and the potential inaccuracy or lack of updates in ccTLD records.

Dual Control: A process using 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, for example, cryptographic key.

ECC: Is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

Email Certificates: Certificates used for encrypting and verifying digital signatures. Generally, there are two separate certificates: one for encryption and one for signature verification.

EMVCo: EMVCo manages, maintains, and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point-of-sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard, and Visa.

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

- Individuals associated directly with, or through, the agents of the Issuing CA, a business group or client (that is, cardholders, merchants, and employees).
- Organizations (that is, Visa Business Groups, clients or their agents or merchants).
- Devices or applications (for example, servers, client software) to be used by the Issuing CA, business group, 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.

Entity: Any autonomous element or component within the PKI that participates in one form or another, such as managing or using certificates. An Entity can be a CA, RA, Subscriber, Relying Party (RP), and so on.

Failover: The capability to switch from a faulty primary server to a backup server either manually or automatically.

FIPS 140-2: Federal Information Processing Standard 140-2 (FIPS 140-2) is a standard that describes US Federal government requirements that information technology (IT) products should meet for Sensitive, but Unclassified (SBU) use. The standard published by the National Institute of Standards and Technology (NIST), has been

adopted by the Canadian Government's Communication Security Establishment (CSE), and might be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard providing different levels of security, and in the higher levels, have different documentation requirements.

FIPS 140-3: Federal Information Processing Standard 140-3 (FIPS 140-3) is a standard that describes US Federal government requirements that information technology (IT) products should meet for Sensitive, but Unclassified (SBU) use. FIPS 140-3 Security Requirements for Cryptographic Modules supercedes FIPS 140-2.

FIPS 180-4: Standard specifying the Secure Hash Algorithm for SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256 for computing a condensed representation of a message or a data file.

Integrity: It ensures 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.

Issuer Public Key: Issuer Public Key (IPK) is a Visa Smart Debit/Credit (VSDC) PKI-generated digital certificate.

Key: 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.

Key Pair: Often referred to as a public/private key pair. One key is used for encrypting (or digitally signing) and the other key is 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.

Non-repudiation: Protection against the denial of the transaction or service or activity occurrence.

Online Certificate Status Protocol: Online Certificate Status Protocol (OCSP) is a protocol developed by the Internet Engineering Task Force (IETF) (Request for Comment [RFC] 2560) to allow a Relying Party to obtain more timely information regarding the revocation status of a certificate than is possible with CRLs.

Object Identifier: The unique alphanumeric identifier registered under the International Standards Organization (ISO) registration standard to reference a standard object or class.

Operative Commercial Agreement: A contract or other binding legal agreement concerning Visa products and services relevant to use of the Visa PKI.

Intermediate Certificate Authority: An Intermediate CA directly subordinate to a Root CA which has subordinate Issuing CAs.

Issuing Certificate Authority: Within the Visa PKI, Issuing CAs are the lowest level of the hierarchy, and only issue End- Entity certificates. They are subordinate to the Intermediate CAs and to the Root CAs.

PKCS #1: Standard that provides recommendations for the implementation of public-key cryptography based on the Rivest, Shamir, Adelman (RSA) algorithm, covering the following aspects, such as:

- Cryptographic primitives
- Encryption schemes
- Signature schemes

PKCS #7: A cryptographic message format or syntax managed and edited by RSA Laboratories. A standard describing 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.

PKCS #10: 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.

PKIX: The Public Key Infrastructure (X.509) or PKIX is an Internet Engineering Task Force (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 developing new standards for use of X.509-based PKI in the Internet.

Public Key Infrastructure Personnel: PKI personnel are generally employees associated with the operation, administration, and management of a CA or RA.

Policy: 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.

PrintableString: 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 ' () + , - . / : = ?.

Private Key: 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 used for digitally signing documents, uniquely authenticating an individual, or decrypting data that was encrypted with the corresponding public key.

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

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

Public Key: The community verification key for digital signature and the community encryption key for encrypting information to a specific End-Entity.

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

Re-Key: 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.

Relative Distinguished Name: A Distinguished Name (DN) is made up of a sequence of Relative Distinguished Names (RDNs). The sequences of RDNs are separated by commas (,) or semicolons (;). 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, and c=US".

RDNs would be:

RDN => cn=Road Runner RDN => ou=bird

RDN => on=mammal RDN => c=US

Relying Party: 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. The RPs within the Visa PKI must have a valid business relationship with Visa and be contractually bound to comply with the Visa By-Laws, Operating Regulations, policies, or operative commercial agreement.

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

Repository: A place or container where objects are stored. A data repository is a 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.

Revocation: In PKI, revocation is the action associated with revoking a certificate. Revoking a certificate is to make the certificate invalid before its normal expiration. The CA that issued the certificate is the entity that revokes a certificate. The revoked status is usually published on a CRL and/or posted on an Online Certificate Status Protocol (OCSP) responder.

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

Sanitization: The process of removing data from storage media such that there is reasonable assurance that the data cannot be retrieved and reconstructed. See National Institute of Standards and Technology (NIST) Special Publication SP800-88.

Sensitive: 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. This is equivalent to the Visa Confidential classification.

Signature Verification Certificate: 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.

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

Subscriber: 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 certificate 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 CAs.

Subscriber Agreement: 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.

Suspension: In PKI, revocation is the action associated with suspending a certificate. Suspending a certificate makes 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 CAs CRLs as 'on hold' and treated by RPs as revoked. At the end of the suspension period, the certificate will be reinstated or revoked. The CA that issued the certificate is the entity that suspends a certificate. The suspended status is usually published on a CRL and/or posted on an Online Certificate Status Protocol (OCSP) responder. Suspending a certificate can potentially avoid an unnecessary or unwarranted revocation.

System: One or more pieces of equipment or software that stores, transforms, or communicates data.

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

TLS Client Certificate: Certificate used to verify the authentication of an End-Entity to a server when a connection is being established through a Secure Socket Layer/Transport Layer Security (SSL/TLS) session (secure channel).

TLS Server Certificate: Certificate used to verify the authentication of a web or application server to the End-Entity (client) when a connection is being established through a Secure Socket Layer/Transport Layer Security (SSL/TLS) session (secure channel).

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

User Notice Qualifier: A User Notice Qualifier in an X.509 certificate intended for display to an RP when the certificate is used.

UTF-8String: Unicode Transformation Format (8-bit) UTF-8 is a type of Unicode, which is a character set supported across many commonly used software applications and operating systems. UTF (8 bit) 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 that universal characters/foreign characters are supported. After 31st December, 2003, all certificates were required to use UTF8String encoding for subject names.

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

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

- End-Entities (that is, individuals associated directly with, or through, the agents of the Visa Regional Business Units, clients, or their agents)
- CAs (Regional Business Units or clients only)

Visa Public Key Infrastructure: This is an X.509 Public Key Infrastructure (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 CAs that issue certificates to Subscribers (that is, End-Entities or other CAs) within the hierarchy. The term Visa PKI is used to refer to all of the Subscribers from the Root CA all the way down to the lowest level End-Entity.

Visa Products and Services: Visa programs that are associated with the Visa-Owned Mark. These include both the products and the underlying services operated by Visa or its agents that are used to support these products.

Visa Smart Debit/Credit: Visa's chip-based payment program.

Vulnerability: Weaknesses in a safeguard or the absence of a safeguard.

X.500: Specification of the directory service required to initially support X.400 email but also commonly used by other applications.

X.501 PrintableString: 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) ' () + , - . / : = ?.

X.509: An International Organization for Standardization (ISO) standard that describes the basic format for digital certificates.

1.6.2. Acronyms

Acronym	Spelled Out Form
BIN	Bank Identification Number used for VSDC PKI processing
BRP	Business Recovery Plan
Business Group	Visa designation for distributed business locations
CA	Certificate Authority
Client	A financial institution, processor, or acquirer that has a service agreement with Visa
CP	Certificate Policy
CPS	Certification Practice Statement
CRF	Cryptographic Review Forum
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAS Application	Extended Access Server application
EAL	Evaluation Assurance Level
ECC	Elliptic curve cryptography
EMV	EuroPay, MasterCard, Visa chip card specification
FIPS	Federal Information Processing Standard
HSM	Host Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
Information Delivery	Visa's Online PKI certificate authorities VICA1 and VICA2 have been deprecated and succeeded by Internal Issuing CA (VICA3) and External Issuing CA (VICA4) respectively
IPK	Visa Smart Debit/Credit formatted Issuer Public Key certificate

Acronym	Spelled Out Form
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
OCSF	Online Certificate Status Protocol
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure Extensions
RA	Registration Authority
RA Manager	Business Group PKI management support personnel
Requester	An authorized member of an approved Visa client, processor, or acquirer who may request a certificate
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SHA	Secure Hash Algorithm
Smart Card	Electronic identity and authorization card used by Information Delivery Vectors to access and approve certificate requests
Subscriber	See Requester
TLS	Transport Layer Security
Tracking Number	A Business Group number system used to track submitted certificates for the VSDC PKI request process
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
Vettor	Visa employee or contractor who processes a certificate request
Vettor Agreement Statement	Annual form signed by the Vettor attesting to his/her responsibilities as a Vettor
VOL Application	Visa Online access application
VSDC	Visa Smart Debit/Credit
VSDC PKI	Visa Smart Debit/Credit Online PKI

1.6.3. References

- National Institute of Technology (NIST) Special Publication SP800-88 Rev-2.
- Internet Engineering Task Force (IETF) Public Key Infrastructure Extensions (PKIXs) Internet X.509 PKI Certificate Policy and Certification Practice Statement Framework (also known as RFC3647).
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

1.6.4. Conventions

The document conventions used in this guide are shown in the following table.

Table 1–1: Document Conventions

Document Convention	Purpose In This Guide
Bold	Used for:
<i>Italics</i>	Used for:
NOTE:	Gives more information about the preceding topic.
IMPORTANT	Highlights important information in the text.
EXAMPLE	Helps to support or explain a general statement.
n/a	Stands for <i>not applicable</i> . Also used to indicate that there is not any information.
Courier typeface	Used for email addresses and for URLs.
Letter Gothic	Used to recreate screen captures and sample report layouts.
”text in quote marks”	Used to refer to section names in a chapter.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

An electronic copy of the Visa Certificate Policy (CP) is to be made available on a 24x7 basis at <https://visawiki.trusted.visa.com/spaces/APC/pages/2141831305/PKI> or by emailing a request for an electronic copy to the Chairman of the Visa Cryptographic Review Forum (CRF), as described in Chapter 1, INTRODUCTION.

A Certificate Authority (CA) should have at least one certificate repository, and one certificate status repository. A repository may or may not be on the same hosting system as the CA, and either certificates or Certificate Revocation Lists (CRLs) may be published to a remote repository or an Online Certificate Status Protocol (OCSP) responder. CRL should be published to a Visa website.

2.2. Publication of Information

The Distribution Point (DP) field within each digital certificate identifies the publicly accessible location where the certificate status information is published in accordance with "Confidentiality of Business Information" and "Privacy of Personal Information".

Online Certificate Status Protocol (OCSP) responders and the CRL publication should be in accordance with Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.

A CA should publish certificate status information as specified by the Visa CPS.

With the exception of the Visa CP, Visa may withhold the security controls and procedures related to the CA.

2.3. Time or Frequency of Publication

Visa reviews and update the CP for required compliance changes. Any changes to the CP should be submitted to the CRF for approval as described in "Policy Administration".

Certificate information should be distributed and/or published after issuance as specified in the Visa CPS. The Visa CP is published in accordance with "Amendments".

Subscriber Agreements or Relying Party Agreements, if applicable, are published as required.

2.4. Access Controls on Repositories

RP's may be given access to certificate status information such as CRLs or by OCSP.

Certificate status information should be distributed and/or published as defined in the Visa CPS and should be in accordance with "CRL Issuance Frequency".

3. IDENTIFICATION AND AUTHENTICATION

The certificate request should be submitted by a Subscriber on his own behalf or on the behalf of the Visa organization, device, or application that uses the certificate.

This chapter describes the requirements for authentication of the Subscriber.

3.1. Naming

3.1.1. Types of Names

Each certificate should have a name for the Subscriber in the certificate Distinguished Name (DN) field. The DN cannot be blank and should use printable characters.

Subscribers may be required to use other subject name fields or attributes including:

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

The Visa Certification Practice Statement (CPS) defines the DN requirements for Subscribers.

Distinguished Names Restrictions

The name by which a Subscriber is known to Visa, Visa regional business groups or Visa client should be used.

Subscribers cannot use fictitious names.

The Visa CPS may specify additional structure to the naming convention such as including a Visa business group or Visa client name.

Certificates that contain wildcard characters ("wildcard certificates") may be signed with the following restrictions in accordance to Section 3.2.2.6, Wildcard Domain Validation:

- The naming convention of *.*.com is used (for example, *.VOL.VISA.COM).
- The application processes transactions at multiple geographic locations where "application session stickiness" is required (for example, active/active at multiple data centers).
- Not more than 30 servers or containers can use a single wildcard certificate.
- Certificates that contain a domain name not owned by Visa ("foreign entity certificates"), for example, server_name.BankX.com, may be signed and requires signed written permission by an authorized officer from the company.

3.1.2. Need for Names to Be Meaningful

3.1.3. Anonymity or Pseudonymity of Subscribers

3.1.4. Rules for Interpreting Various Name Forms

3.1.5. Uniqueness of Names

3.1.6. Recognition, Authentication, and Role of Trademarks

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

A certificate request should be a self-signed certificate (for example, Public Key Cryptographic Standard (PKCS #10) to demonstrate possession of a private key.

3.2.2. Authentication of Organization and Domain Identity

A Subscriber enrollment process should be made by a person authorized to act on behalf of the organization.

The enrollment process should include details about the Subscriber as requested by the Certificate Authorities (CAs). The details should be provided in a secure manner.

The CAs or Registration Authorities (RAs) should verify the identity of the Subscriber and the Visa business relationship. Records of the details used for the Subscriber's identification should be kept for at least ninety (90) days.

3.2.2.1. Identity

3.2.2.2. DBA/Tradename

3.2.2.3. Verification of Country

3.2.2.4. Validation of Domain Authorization or Control

3.2.2.4.1. Validating the Applicant as a Domain Contact

3.2.2.4.2. Email, Fax, SMS, or Postal Mail to Domain Contact

3.2.2.4.3. Phone Contact with Domain Contact

3.2.2.4.4. Constructed Email to Domain Contact

3.2.2.4.5. Domain Authorization Document

3.2.2.4.6. Agreed-Upon Change to Website

3.2.2.4.7. DNS Change

3.2.2.4.8. IP Address

3.2.2.4.9. Test Certificate

3.2.2.4.10. TLS Using a Random Value

3.2.2.4.11. Other Methods

3.2.2.4.12. Validating Applicant as a Domain Contact

- 3.2.2.4.13. Email to DNS CAA Contact**
- 3.2.2.4.14. Email to DNS TXT Contact**
- 3.2.2.4.15. Phone Contact with Domain Contact**
- 3.2.2.4.16. Phone Contact with DNS TXT Record Phone Contact**
- 3.2.2.4.17. Phone Contact with DNS CAA Phone Contact**
- 3.2.2.4.18. Agreed-Upon Change to Website v2**
- 3.2.2.4.19. Agreed-Upon Change to Website – ACME**
- 3.2.2.4.20. TLS Using ALPN**
- 3.2.2.4.21. DNS Labeld with Account ID - ACME**
- 3.2.2.4.22. DNS TXT Record with Persistent Value**
- 3.2.2.5. Authentication for an IP Address**
 - 3.2.2.5.1. Agreed-Upon Change to Website**
 - 3.2.2.5.2. Email, Fax, SMS, or Postal Mail to IP Address Contact**
 - 3.2.2.5.3. Reverse Address Lookup**
 - 3.2.2.5.4. Any Other Method**
 - 3.2.2.5.5. Phone Contact with IP Address Contact**
 - 3.2.2.5.6. ACME "http-01" method for IP Addresses**
 - 3.2.2.5.7. ACME "tls-alpn-01" method for IP Addresses**

3.2.2.6. Wildcard Domain Validation

Before issuing a Wildcard Certificate, the CA should establish that the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled[†] or public suffix, CAs should refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (E.g. CAs should NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.).

3.2.2.7. Data Source Accuracy

3.2.2.8. CAA Records

3.2.2.9 Multi-Perspective Issuance Corroboration

3.2.3. Authentication of Individual Identity

Authorized individuals of Visa business groups, Visa clients, employees, or merchants may submit a request to become a Subscriber to a CA.

Individuals should only be End-Entity Subscribers. The Subscriber is responsible for:

- Generating a request that meets Visa Public Key Infrastructure (PKI) requirements as stated in this CP.
- Delivering an authenticated request to the RA in a secure manner (for example, Secure Multipurpose Internet Mail Extension (S/MIME) or equivalent protected file).

The RA has the responsibility, on behalf of a CA, for:

- Completing the verification and authorization requirements as stated in the Visa Vettor GuideTemplate.
- Verifying successful completion of the prerequisites that should be performed before the generation of the key pair and certificate request.
- Authenticating the entity submitting the request in accordance with the identification and authentication procedures specified for the type of certificate and/or for the Visa product or service with which the certificate is intended to be used.
- Verifying that the certificate request has been transferred from the Subscriber to the RA in a secure manner as defined by the Visa CPS.
- Processing the certificate request, along with the appropriate documentation, to the CA as defined by the Visa CPS.

The CA or RA should keep a record of the certificate processing documentation for at least two ninety (90) days.

3.2.4. Non-Verified Subscriber Information

Non-verified subscriber information is any certificate information not validated through the requirements set forth in the *Visa Global PKI - Vettor Operations Guide*.

3.2.5. Validation of Authority

Authorization to request a certificate is required to be an official appointment (for example, company/organization letter signed by an organizational authority).

Prior to using any data source as a Reliable Data Source, the Vettor should evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The vettor SHOULD consider the following during its evaluation:

- The age of the information provided.
- The frequency of updates to the information source.
- The data provider and purpose of the data collection.
- The public accessibility of the data availability.
- The relative difficulty in falsifying or altering the data.

Databases maintained by the CA Vettor, do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements.

Authenticity of the Applicant Representative's certificate request is verified as stated in the Visa Global PKI Vettor Operations Guide Template.

3.2.6. Criteria for Interoperation or Certification

Cross certification within CAs or with external CAs is not supported. The Visa PKI hierarchy is a closed PKI.

3.3. Identification and Authentication for Re-Key Requests

3.3.1. Identification and Authentication for Routine Re-key

Not applicable.

3.3.2. Identification and Authentication for Re-key After Revocation

Not applicable.

3.4. Identification and Authentication for Revocation Requests

CAs or RAs should authenticate a request for revocation of a certificate in the same manner as a certificate request.

The CAs or RAs should keep a record of the type and details of the revocation request, including the identity and authentication of the person making the request, for at least ninety (90) days.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

An application for a certificate does not oblige a Certificate Authority (CA) to issue a certificate.

Required Information for a Certificate Request Subscriber information should be complete, validated, and accurate with full disclosure of required information in connection with a certificate request.

Subscribers Agreement or Equivalent Documentation Subscribers registering for a Visa product or service using a Visa-issued certificate should be required to consent to a Subscribers Agreement or equivalent prior to certificate issuance.

4.1.1. Who Can Submit a Certificate Application

The following list of roles is authorized to submit certificate applications:

- An authorized representative of an Organization or entity that has a current business relationship with Visa, Inc.
- Any individual who is the subject of the certificate.
- Any authorized representative of an Organization or entity.
- Any authorized representative of a CA.
- Any authorized representative of a Registration Authority (RA).

4.1.2. Enrollment Process and Responsibilities

End-user Certificate Subscribers consent to the relevant Subscriber Agreement and complete the enrollment process by:

- Completing the relevant Certificate Application form with true and correct information, generating or arranging to have generated a key pair.
- Delivering an owned public key, directly or through an RA, to Visa CAs.
- Demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to Visa.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

4.2.2. Approval or Rejection of Certificate Applications

A CA or an RA should notify a Subscriber that the request has been rejected or accepted. If accepted, the CA should create a certificate and provide the Subscriber with access to the certificate.

4.2.3. Time to Process Certificate Applications

The processing time for certificate requests is described in the Visa Certification Practice Statement (CPS).

4.2.4. Certificate Authority (CAA) record

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

A certificate is created and issued following the approval of a certificate request by authorized individuals or following receipt of an RA's request to issue the Certificate. Certificates are issued based on the information in a certificate request, validation of the requestor and information provided, and approval of the certificate request.

4.3.1.1. Manual Authorization of Certificate Issuance for Root CAs

Certificate issuance by the Root CA should require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.1.2 Linting of to-be-signed Certificate Content

4.3.1.3 Linting of Issued Certificates

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Visa, either directly or through an RA, notifies the Subscribers that their certificates are available. Certificates are made available to end-user Subscribers, either by allowing them to download them from a web site or through a message containing the Certificate sent to the Subscriber.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

By accepting and using the certificate, the Subscriber agrees to comply with the terms of any policies referenced within the Certificate Policies (CPs) field of the certificate.

4.4.2. Publication of the Certificate by the CA

A CA is responsible for repository and publication functions. A CA should publish certificates in a repository based on the certificate publishing practices defined in the Visa CPS.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

A CA should only use its private key to sign certificates and Certificate Revocation Lists (CRLs) for use with production implementations of Visa products and services. A CA should not transfer its private key from the platform on which it was generated to another platform except for business recovery or load balancing purposes, unless it obtains prior written permission from the Visa Cryptographic Review Forum (CRF). A CA should use commercially reasonable efforts to ensure that issued certificates and associated private and public key pairs are used only for functions to access and operate Visa products and services.

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

The Subscriber should only use production certificates issued by an Issuing CA for access to Visa products and services. The certificates should not be used in a test environment unless a variance is obtained from the CRF and the appropriate CA prior to their use. A separate process is available for requesting test certificates.

Publisher Certificate and Usage

A publisher certificate is a certificate with code or document signing extensions. Publisher certificates private keys should be stored with a tamper-resistant security module, for example, smart card.

4.5.2. Relying Party Public Key and Certificate Usage

It is recommended that a Relying Party (RP) verify that a Subscriber's certificate is appropriate for the application prior to use.

4.6. Certificate Renewal

4.6.1. Circumstance for Certificate Renewal

4.6.2. Who May Request Renewal

4.6.3. Processing Certificate Renewal Requests

4.6.4. Notification of New Certificate Issuance to Subscriber

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

4.6.6. Publication of the Renewal Certificate by the CA

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

4.7. Certificate Re-Key

4.7.1. Circumstance for Re-Key

4.7.2. Who May Request Certification of a New Public Key

4.7.3. Processing Certificate Re-Keying Requests

4.7.4. Notification of New Certificate Issuance to Subscriber

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

4.7.6. Publication of the Re-Keyed Certificate by the CA

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

4.8. Certificate Modification

Certificate modification is not supported.

4.8.1. Circumstance for Certificate Modification

4.8.2. Who May Request Certificate Modification

4.8.3. Processing Certificate Modification Requests

4.8.4. Notification of New Certificate Issuance to Subscriber

4.8.5. Conduct Constituting Acceptance of Modified Certificate

4.8.6. Publication of the Modified Certificate by the CA

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

A certificate should be revoked or otherwise invalidated under any of the following circumstances:

- When a Subscriber fails to comply with obligations set forth in the Visa Certificate Policy (CP) or this Visa CPS.
- When the basis for any information in the certificate changes.
- When a change in the business relationship under which the certificate was issued.
- When a Subscriber is no longer participating in the Visa product or service for which the certificate was issued.
- Upon suspected or known compromise of the private key or the media holding the key.
- Upon termination of a Subscriber.
- When the certificate has been issued to an ineligible Subscriber.
- When a Subscriber no longer needs access to Visa products or services

4.9.1.1. Reasons for Revoking a Subscriber Certificate

Refer to CPS for details.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

Refer to CPS for details.

4.9.2. Who Can Request Revocation

The revocation of a certificate should only be requested by:

- The Subscriber to whom the certificate is issued. If requesting revocation, the Subscriber to whom the certificate is issued should notify the Business Group/Application Vettor.
- An authorized client or supervisor or manager on behalf of a Subscriber.
- An RA associated with the Issuing CA.
- The Issuing CA.

4.9.3. Procedure for Revocation Request

A Certificate Authority (CA) should make certificate revocation data available to Subscribers or RPs. The notice of revocation should be posted to a Certificate Revocation List (CRL) within the time limits stated in this Visa CPS. The address of the CRL should be defined in the certificate.

All requests for revocation should be submitted to the Certificate Authority (CA) or RA or vettors authorized to act on behalf of subscribers and Visa's clients.

The revocation request and any resulting actions taken by the Certificate Authority (CA) should be recorded and retained for a minimum of ninety (90) days.

Suspected Private Key compromise, fraud, or any matter related to certificate compromise or fraud should be reported to PKIPolicy@visa.com.

Visa responds to revocation requests and other requests on a 24x7 basis.

Subscribers should follow the Certificate Revocation procedures in the Visa Certificate Policy located at <https://visawiki.trusted.visa.com/spaces/APC/pages/2141831305/PKI>.

Suspension of Certificates Pending Revocation Validation

The Certificate Authority (CA) or RA may, at its discretion, suspend a certificate immediately upon notification of a revocation request.

Revocation Processing Time frame

The CA should process a revocation request within the time period, as defined in the Visa CPS.

4.9.4. Revocation Request Grace Period

The revocation grace period is the maximum period available within which the Subscriber should make a revocation request upon suspicion of compromise. The grace period cannot extend beyond one (1) Visa business day for the relevant geographical location.

A CA reserves the right to not re-issue a certificate if the grace period was not respected (that is, negligence on behalf of the Subscriber).

4.9.5. Time Within Which Certificate Authority Must Process the Revocation Request

The period of time between the receipt of a request for certificate revocation and the beginning of the investigation process for a certificate problem or certificate revocation will be a maximum of 24 hours for the active issuing CA.

Revocation entries on a CRL or OCSP Response should NOT be removed until after the Expiry Date of the revoked Certificate.

S/MIME certificates are revoked upon due process through HR notification to the relevant parties.

4.9.6. Revocation Checking Requirement for Relying Parties

RPs should check the status of certificates in the certificate validation chain against current CRLs before their use, including the authenticity and integrity of CRLs. If the RP stores a copy of the CRL, they should retrieve a 'fresh' CRL at least daily.

Online Certificate Status Protocol (OCSP) responders are available on the URL: <https://ocsp.visa.com/ocsp>

4.9.7. CRL Issuance Frequency

A CA should issue CRLs with the most current certificate status of issued certificates. The CRL issuance frequency is specified in the Visa CPS.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. Online Revocation/Status Checking Availability

Online revocation and other certificate status information are available 24x7 through a web-based repository and OCSP. OCSP certificate status information is also provided to those who contact the OCSP services to check certificate status. The URL for the relevant OCSP Responder is communicated in the certificate.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds should be equal to one hour, and a difference of 86,400 seconds should be equal to one day, ignoring leap-seconds.

A certificate serial is “assigned” if:

- a Certificate or Precertificate with that serial number has been issued by the Issuing CA; or
- a Precertificate with that serial number has been issued by a Precertificate Signing Certificate, as defined in Section 7.1.2.4, associated with the Issuing CA.

A certificate serial is “unassigned” if it is not “assigned”.

The following should apply for communicating the status of Certificates and Precertificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod.

4.9.10 Online Revocation Checking Requirements

A relying party should confirm the validity of a certificate in accordance with Section 4.9.6 before relying on the certificate.

4.9.11. Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements Related to Key Compromise

Visa makes reasonable efforts to notify potential RPs if it discovers or has a reason to believe that there has been a compromise of the private key.

4.9.13. Circumstances for Suspension

A certificate may be suspended or revoked whenever any of the conditions listed in “Circumstance for Certificate Renewal” are suspected or known. A CA may, at its discretion, suspend a certificate rather than revoke it immediately, pending validation of the revocation request.

4.9.14. Who Can Request Suspension

The suspension of a certificate can only be requested by:

- The Subscriber to whom the certificate is issued. If requesting suspension, the Subscriber to whom the certificate is issued should notify the Business Group/Application Vettor.
- An authorized client or supervisor or manager on behalf of a Subscriber.
- An RA associated with the Issuing CA.

4.9.15. Procedure for Suspension Request

With respect to a certificate's suspension, the procedures and requirements are equivalent to those for revocation defined in “Procedure for Revocation Request” to “CRL Issuance Frequency”.

4.9.16. Limits on Suspension Period

When a certificate is suspended pending verification of a revocation request, the suspension period should be appropriate to validate the revocation request. At the end of the suspension period, the CA should 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

Certificate status information is available through CRL, and OCSP responder as described in Section 4.9.6.

Revocation entries on a CRL or OCSP response should NOT be removed until after the expiry date of the revoked Certificate.

4.10.2. Service Availability

CRL and OCSP will provide a response time of ten seconds or less under normal operating circumstances. The Certificate status service is available on a 24x7 basis.

4.10.3. Optional Features

OCSP is an optional status service feature that is not available for all certificate types and is specifically enabled for all SSL certificates.

4.11. End of Subscription

A Subscriber's subscription service ends if:

- Its certificate expires.
- Its certificate is revoked.
- The business relationship with Visa expires.
- The business relationship with Visa is terminated.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

The CA private key(s) should not be escrowed.

End-Entity Key Escrow and Recovery Policy and Practices should be followed for S/MIME certificates

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Corporate End-Entity certificates for email encryption may be recovered by processes as defined in the Visa CPS. Any other End-Entity private key(s) should not be escrowed.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

The CA should develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to the CA by law.
6. The Certificate Management Process should include:
7. Physical security and environmental controls;
8. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
9. Network security and firewall management, including port restrictions and IP address filtering;
10. User management, separate trusted-role assignments, education, awareness, and training; and logical access controls, activity logging, and inactivity time-outs to provide individual accountability.
11. The CA's security program should include an annual Risk Assessment that:
12. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
13. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
14. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.
15. Based on the Risk Assessment, the CA should develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan should include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan should also take into account then-available technology and the cost of implementing the specific measures, and should implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1. Physical Security Controls

The Certificate Authority (CA) facilities should provide the physical security controls as outlined in the Visa Certification Practice Statement (CPS).

5.1.1. Site Location and Construction

The following requirements and procedures should be implemented:

- The access control systems should:
 - Be inspected at least semi-annually by qualified personnel.
 - Have documentation retained for at least ninety (90) days.
- Access control and monitoring systems should be supported with an Uninterruptable Power Supply (UPS) system. The UPS system should:
 - Be inspected at least annually.
 - Have documentation retained for at least ninety (90) days.

5.1.2. Physical Access

The physical access controls are defined in the Visa CPS.

5.1.3. Power and Air Conditioning

The CA facility management should ensure that the power and air conditioning are sufficient to support the operation of the CA system.

5.1.4. Water Exposure

The CA facility management should ensure that water exposures, fire prevention and protection, and other environmental controls are sufficient to support the operation of the CA system.

5.1.5. Fire Prevention and Protection

The CA facility management should ensure that the fire prevention and protection are sufficient to support the operation of the CA system.

5.1.6. Media Storage

The PKI should ensure that the storage media used by a CA system is protected from environmental threats such as temperature, humidity, and magnetic activity.

5.1.7. Waste Disposal

A CA should ensure the destruction or sanitization of confidential media.

5.1.8. Off-site Backup

A CA should ensure that the business recovery site maintains a comparable level of security as the primary site.

5.2. Procedural Controls

5.2.1. Trusted Roles

CA administrators should be individually accountable for their actions by a combination of the following physical, electronic, and policy controls:

- Restricted access to facility. Entry and exit should be controlled and monitored.
- Audit logs should record the following:
 - The administrator's activities of logging in and logging out of the operating system.
 - The administrator's activities of logging in and logging out of the CA application.
 - Certificate creation, issuance, suspension, revocation, and changes by the CA.
- Policy, procedural, and technical controls that require dual access.

Registration Authority Trusted Roles

The Visa CRF requires that the Registration Authority (RA) personnel understand their responsibility for the identification and authentication of prospective Subscribers and that they perform the following functions:

- Acceptance of certificate requests, certificate changes, certificate revocation requests, and key recovery requests (if applicable).
- Verification of a Subscriber's identity and authorizations.
- Secure transmission of applicant information to the issuing CA.
- Provide shared secrets, as required, for authenticating Subscribers.
- RA agents (vectors) issuing TLS (except-S/MIME) certificates should undergo annual compliance to affirm their knowledge and responsibilities.

5.2.2. Number of Individuals Required Per Task

The Visa PKI should have a verification process that provides an oversight of activities performed by privileged CA role holders.

The activities include issuing certificates, generating keys, and administering the CA configuration settings.

5.2.3. Identification and Authentication for Trusted Roles

CA personnel should have their identity and authorization verified before they are:

- Granted physical access to a CA facility.
- Given logical access to a CA system.
- Given a certificate for the performance of their CA operation's role. Each certificate:
 - should be directly attributable to an individual.
 - should not be shared.
 - should be restricted to actions authorized for that role through the use of the CA software, operating system, and procedural controls.

5.2.4. Roles Requiring Separation of Duties

5.3. Personnel Controls

Personnel performing duties with respect to the operation of a CA (for example, PKI administrators, key custodians, and vectors) should:

- Be bound by the terms and conditions of the position they support.
- Not disclose sensitive CA information or Subscriber information.
- Regional Vector personnel are required to validate their understanding of their job function through a signed Vector Agreement form as defined in Appendix A of the Visa Certification Practice Statement (CPS).

5.3.1. Qualifications, Experience, and Clearance Requirements

A CA should require that personnel performing duties with respect to the operation of a CA have sufficient training, qualifications, and experience in PKI. CA personnel should also meet Visa personnel security requirements.

5.3.2. Background Check Procedures

Background checks should be performed on the CA operations personnel in accordance with Visa standard hiring practices and any relevant country legal restrictions.

5.3.3. Training Requirements and Procedures

The PKI should provide comprehensive training for PKI personnel performing duties with respect to the operation of a CA. Such training should include at least:

- Information Security and general PKI knowledge.
- CA administration and operation.
- CA business recovery processes.
- Applicable industry and government guidelines.
- Visa Security Compliance training.

The Visa CA maintains records of training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform the duties satisfactorily.

Validation Specialists engaged in Certificate issuance maintain skill levels consistent with the Visa CAs training and performance programs.

The Visa CA documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

The Visa CA requires Validation Specialists to pass an examination, provided by the Visa CA, on the information verification requirements outlined in these requirements.

5.3.4. Retraining Frequency and Requirements

The requirements for training (see "Training Requirements and Procedures") should be kept current to accommodate changes in CA system software and procedures.

Refresher training should be conducted as required, and management should review these requirements periodically.

5.3.5. Job Rotation Frequency and Sequence

When there is job rotation, relevant service account passwords should be changed, and individual credentials should be deleted.

5.3.6. Sanctions for Unauthorized Actions

When there is an actual or suspected unauthorized action by a person performing duties with respect to the operation of a CA, that CA should immediately revoke the person's access to the CA system.

A CA may revoke a certificate when an entity fails to comply with obligations set out in this Visa Certificate Policy (CP) and the Visa CPS. A CA may suspend 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 Controls

A CA should limit contractor access to the CA facility in accordance with the Visa CPS. Contractor personnel should be escorted while in the CA facilities.

5.3.8. Documentation Supplied to Personnel

Visa PKIs should provide access to this Visa CP and Visa CPS to Visa personnel performing duties with respect to the operation of a CA.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

A CA SHOULD record relevant events, successes, and failures related to the security of that CA system in audit log files. Whether electronic or manual, logs should include the date and time of the event and who or what entity (for example, application) caused the event.

A CA SHOULD indicate what information is logged in the Visa CPS. Certificate Authority Physical Security Logs CA physical access events should be recorded as follows:

- Automated mechanisms should exist for logging access.
- Access granting, revocation, and review procedures should be documented.
- Visitors (contractors, maintenance personnel, and so on) to the physically secure environments must should be escorted and should sign an access logbook. This log should be maintained within the physically secure facility. This logbook should 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
- Alarm events should be documented. Under no circumstances can an individual sign-off on an alarm event in which they were involved.
- The use of any emergency entry or exit mechanism should cause an alarm event. An assessment should occur within 24 hours to identify the effect (for example, loss of dual control by authorized individuals) of the use of this mechanism. This assessment should be documented and retained for at least ninety (90) days.
- A process should exist for synchronizing the time and date stamps of the access, intrusion detection, and monitoring (camera) systems to ensure accuracy of the logs. This may be done by either automated or manual mechanisms. If a non-continuous process is used, the process should occur at least quarterly. Documentation of the synchronization should be retained for at least ninety (90) days.

5.4.1.1 Router and Firewall Activities Logs

Logging of router and firewall activities necessary to meet the requirements of Section 5.4.1, should at a minimum include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2. Frequency of Processing Audit Log

At a minimum, a review SHOULD be conducted once in thirty (30) days for online CAs. Significant events should be explained in an audit log summary. Actions taken following these reviews should be documented.

5.4.3. Retention Period for Audit Log

A CA should retain its audit logs for records related to the issuance and any revocation of a certificate for at least ninety (90) days after the certificate is expired.

5.4.4. Protection of Audit Log

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

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

5.4.5. Audit Log Backup Procedures

Audit logs and audit summaries should be backed up or copied daily. For offline CAs, this should occur after each ceremony generation. Timelines for retaining backups should conform to standard commercial and legal requirements. At a minimum, backups should be retained for ninety (90) days for records related to the issuance and/or revocation of a certificate, after the certificate is revoked or has expired.

5.4.6. Audit Collection System (Internal vs. External)

Access to the building, room and/or cage, cabinets, and safes where the CA system components are stored and used should be monitored.

Operating System audit processes should be invoked at system startup and end only at operating system shutdown. The CA system audit processes should be invoked at CA application startup and should end only at CA system shutdown. If the automated audit system has failed and the integrity of the system or confidentiality of the information protected by the system is at risk, the PKI determines whether to suspend CA operations until the problem is resolved.

5.4.7. Notification to Event-Causing Subject

When an event is logged, no notice needs to be given to the individual or entity that caused the event.

5.4.8. Vulnerability Assessments

Events in the audit process are logged to monitor system vulnerabilities and/or compromises. A CA should perform a vulnerability assessment, and action should be taken following these monitored events.

Visa performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats, which could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process.

5.5. Records Archival

Public verification keys contained in digital certificates and confidentiality private keys stored by the issuing CA should be retained for a minimum of ninety (90) days after the expiration of the key material.

5.5.1. Types of Records Archived

Refer to CPS for details of type of records to be archived.

5.5.2. Retention Period for Archive

The minimum retention period for archive data is ninety (90) days, customer-specific information must be disposed of according to Visa Key Controls.

5.5.3. Protection of Archive

See CPS for details.

5.5.4. Archive Backup Procedures

See CPS for details.

5.5.5. Requirements for Time-stamping of Records

See CPS for details.

5.5.6. Archive Collection System (Internal or External)

See CPS for details.

5.5.7. Procedures to Obtain and Verify Archive Information

See CPS for details.

5.6. Key Changeover

Automatic key changeover (renewal) is not supported.

5.7. Compromise and Disaster Recovery

Information related to business recovery of the CA is provided in the Visa CPS and is further described in the CA Business Recovery Plan (BRP).

When there is a compromise of a CA, the CA should notify its Subscribers promptly. Detailed instructions are specified in the Visa CPS.

Steps to be followed are summarized below:

1. Notify the dependent CAs and customers.
2. Revoke certificates associated with the compromised keys (for CAs except VSDC, where revocation is not currently supported).
3. Investigate the compromise.
4. Report results of the investigation and required actions.
5. Implement the actions.
6. Perform key ceremonies for dependent CAs.
7. Issue new certificates.
8. Notify browser vendors (for CAs except VSDC, where revocation is not currently supported).

5.7.1. Incident and Compromise Handling Procedures

Detailed instructions are specified in the Visa CPS.

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data are Corrupted

Local failover capabilities should be implemented to mitigate the loss of computing resources and software or data corruption. When a primary site is inoperable, the BRP See CPS for details. be implemented.

5.7.3. Recovery Procedures After Key Compromise

See CPS for details.

5.7.4. Business Continuity Capabilities after a Disaster

See CPS for details.

5.8. CA or RA Termination

See CPS for details.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Key pair generation should be supported in either hardware or software as stipulated in "Public Key Parameters Generation and Quality Checking".

6.1.1.1. CA Key Pair Generation

Refer to CPS for details on CA key Pair Generation.

6.1.1.2. RA Key Pair Generation

6.1.1.3. Subscriber Key Pair Generation

6.1.2. Private Key Delivery to Subscriber

Subscribers requesting TLS certificates should generate their key pair and retain their private key.

6.1.3. Public Key Delivery to Certificate Issuer

Public keys and certificates may be stored in the Certificate Authority (CA) repository. Delivery of public keys may be in Distinguished Encoding Rules (DERs) encoded (binary or base64) Public Key Cryptography Standard (PKCS) #10 format or EMV format.

6.1.4. CA Public Key Delivery to Relying Parties

Public keys and certificates may be stored in the CAs repository. The CA public key, as part of the certificate, may be delivered to a Subscriber as part of the issuing process. The format may be DERs encoded (binary or base64) or PKCS #7 (binary or base64), with or without chain, or EMV format depending on the Subscriber's requirements as outlined in the Visa Certification Practice Statement (CPS).

6.1.5. Algorithm Type and Key Sizes

Key pairs for Public Key Infrastructure (PKI) TLS certificates should be a minimum of RSA 2048 bits in length or equivalent.

6.1.6. Public Key Parameters Generation and Quality Checking

CA keys should be generated using a random or pseudo-random number generator that is capable of satisfying the statistical tests and the cryptographic module requirements, as defined in Federal Information Processing Standards (FIPS) Publication 140-2 or 140-3, level 3.

End-Entity key pairs for Visa Business Groups, clients, or their agents that are destined for use with Visa products and services should be generated and protected, as described in the relevant Visa product and service documentation.

At a minimum, the key generation requirements should meet the business objectives of the Visa product and/or service.

Key pairs for other entities not listed above may be generated and stored in software or protected by secure cryptographic hardware modules as defined by the Visa CPS.

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

6.2. Private Key Protection and Cryptographic Module Engineering Controls

The Subscriber should protect its private key from disclosure according to the requirements defined by the Visa CPS. The Subscriber is responsible for its private keys.

The private key of an entity should be protected from unauthorized use by a combination of commercially reasonable cryptographic and physical access control mechanisms defined by the Issuing CA and described in the Visa CPS. The level of protection should be adequate to deter a motivated attacker with substantial resources.

If key recovery is implemented, the data encryption private keys used for email encryption should be stored in a password-protected media or in the end-user's smart card or stored by the CA protected by cryptographic hardware.

6.2.1. Cryptographic Module Standards and Controls

CAs digital signature key storage and certificate signing operations should be performed in a secure cryptographic hardware module rated to at least FIPS (FIPS 140-2 or 140-3, Level 3 or Level 4, as appropriate to the device) or otherwise verified to an equivalent level of functionality and assurance.

At a minimum, the key generation and protection should meet the business objectives and requirements of the Visa product and/or service.

6.2.2. Private Key (n out of m) Multi-Person Control

There SHOULD be multiple-person control for CA key generation operations. At a minimum, there SHOULD be multi-person control for operational procedures so that no one can gain control over the CA signing key. The principle of split knowledge and dual control SHOULD be applied as described in "Trusted Roles".

6.2.3. Private Key Escrow

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

Subscriber Digital Signature private keys should not be escrowed.

6.2.4. Private Key Backup

The CAs should back up CA private signing keys in a secure manner to support business recovery operations.

6.2.5. Private Key Archival

Corporate End-Entity key recovery for email encryption may be archived according to documented processes. Other End-Entity private keys should not be archived.

6.2.6. Private Key Transfer into or from a Cryptographic Module

CA keys SHOULD be generated by and in a cryptographic module. CA Private Keys are not exported from the cryptographic module.

6.2.7. Private Key Storage on Cryptographic Module

CA Keys SHOULD be generated and protected by hardware cryptographic modules which have been evaluated to at least FIPS 140-2 or 140-3 Level 3.

6.2.8. Activating Private Keys

6.2.9. Deactivating Private Keys

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

6.2.10. Destroying Private Keys

Upon termination of the use of a private key, over-writing should securely destroy copies of the private key in computer memory and shared disk space. The private keys should be destroyed in accordance with Cryptographic Key Generation and Destruction. See Section 5.14.2.3, "Key Management" in Visa Key Controls. Details of these arrangements are described in the Visa CPS.

6.2.11. Cryptographic Module Rating

Cryptographic Module's used in CA and VA systems SHOULD be FIPS 140-2 or 140-3 certified.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Issuing CAs should retain verification public keys for the period of time defined in the Visa CPS.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Issuing CA private signing keys should expire prior to the CA key that signed the public verification key. If the CA certificate contains a private key usage extension, the expiration date for the private signing key should correspond to the date included in that extension.

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

6.4. Activation Data

If activation data is used to protect any CA private key, it should be unique and unpredictable, and it should be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms.

6.4.1. Activation Data Generation and Installation

6.4.2. Activation Data Protection

6.4.3. Other Aspects of Activation Data

6.5. Computer Security Controls

6.5.1. Computer Security Requirements

Computer security controls for CAs should provide protection from unauthorized access, modification, substitution, insertion, and/or deletion. These controls provide protection to help ensure that any such attempts are prevented or will have a high probability of being detected in a timely manner.

The following functionality for CAs should be provided by the operating system or through a combination of operating systems, CA software, and/or physical safeguards (policies and procedures).

Each CA server should include the following functions:

- Access control to CA services.

- Enforced separation of duties for CA administrative roles.
- Identification and authentication of CA administrative roles and associated identities.
- Use of cryptography for session communication and database security.
- Archival of CA and End-Entity history and audit data.
- Audit of security-related events.
- Trusted path for identification of PKI roles and associated identities.
- Recovery mechanisms for keys and the CA system.
- Multi-factor authentication for certificate issuing accounts.

6.5.2. Computer Security Rating

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Visa PKIs should 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 should support the design and development process.

If a CA uses Linting software developed by third parties, it SHOULD monitor for updated versions of that software and plan for updates no later than three (3) months from the release of the update.

The CA MAY perform Linting on the corpus of its unexpired, un-revoked Subscriber Certificates whenever it updates the Linting software.

6.6.2. Security Management Controls

A formal configuration management methodology should be used for installation and ongoing maintenance of a CA system. CA software, when first loaded, should 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.
- Is the intended version.

The PKI operating environment should provide a commercially reasonable mechanism to verify the integrity of the CA software.

The PKI operating environment should have commercially reasonable mechanisms and policies in place to control and monitor the configuration of the CA system.

6.6.3. Life Cycle Security Controls

6.7. Network Security Controls

The Visa Root CAs are not connected to any network, which eliminates a threat of attack through open or general-purpose networks.

The online Issuing CAs should use commercially reasonable efforts to protect their servers from attack through any open or general-purpose networks. The protection should be provided through 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 and/or service.

Those protocols and commands required for the protection of the CAs are defined in the Visa CPS.

6.8. Time-Stamping

Certificates, CRLs, and Online Certificate Status Protocol (OCSP) responders contain time and date information. Time information does not need to be cryptographic-based.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Visa Smart Debit/Credit (VSDC) certificates should conform to the EMV specification.

7.1. Certificate Profile

7.1.1. Version Number(s)

Certificate Authorities (CAs) should issue X.509 Version 3 certificates based on the Internet Engineering Task Force (IETF) Public Key Infrastructure Extensions (PKIX) Certificate, and Certificate Revocation List (CRL) Profile as defined in RFC 5280 and its successors. The PKI End-Entity software should support all the base (non-extension) X.509 fields as well as any certificate extensions as defined in Visa Certification Practice Statement (CPS).

Base Certificate Format

The Base Certificate Format conforms to the Internet Engineering Task Force (IETF) Public Key Infrastructure Extensions (PKIX) RFC 5280, "Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile".

The following table shows the base certificate fields supported. Additional extensions are allowable if required.

Table 7–1: Supported Base Certificate Fields

Certificate Field	Description
Version	3
Serial Number	Unique non-sequential identifying number that exhibits at least 64 bits of entropy for this certificate assigned by the Public Key Infrastructure (PKI).
Signature	CRF-approved algorithms.
Issuer	The Visa CA should conform with "Issuer Information".
Validity	Start and expiration dates and times of the certificate.
Subject	Fully qualified domain name (DN) (X.500) of the subject, as per "Types of Names".
Subject public key information	The value of the public key for the subject along with an identifier of the algorithm with which this public key is to be used.

7.1.2. Certificate Content and Extensions

Extensions used by the CAs should be published in the Visa CPS. Critical extensions should be interpreted as defined in PKIX.

7.1.2.1. Root CA Certificate Profile

Refer to CPS for details.

7.1.2.2. Cross-Certified Subordinate CA Certificate Profile

Refer to CPS for details.

7.1.2.3. Technically Constrained Non-TLS Subordinate CA Certificate Profile

Refer to CPS for details.

7.1.2.4. Technically Constrained Precertificate Signing CA Certificate Profile

Refer to CPS for details.

7.1.2.5. Technically Constrained TLS Subordinate CA Certificate Profile

Refer to CPS for details.

7.1.2.6. TLS Subordinate CA Certificate Profile

Refer to CPS for details.

7.1.2.7. Subscriber (Server) Certificate Profile

Refer to CPS for details.

7.1.2.8. OCSP Responder Certificate Profile

Refer to CPS for details.

7.1.2.9. Precertificate Profile

7.1.2.10. Common CA Fields

Refer to CPS for details.

7.1.2.11. Common Certificate Fields

Refer to CPS for details.

7.1.3. Algorithm Object Identifiers

The CAs should use, and the Subscribers and Relying Parties (RPs) should support for signing and verification, the following:

- RSA (2048 bit modulus or higher unless approved by the Visa CRF) or equivalent algorithm in accordance with Public Key Cryptography Standard (PKCS)#10. Nist Curves P-256 and P-384.
- Secure Hash Algorithm (SHA-1 SHA-2) algorithm in accordance with Federal Information Processing Standard (FIPS) Publication (PUB) 180-4 2012.
- Post-Quantum Cryptography (PQC) algorithm, including NIST-selected standards such as ML-DSA for digital signatures and ML-KEM for key establishment, following the latest NIST PQC specifications as published in the final standards.

CA's should NOT issue any SSL/TLS Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. CA's MAY issue Root CA certificates or Subordinate CA Certificates that are Cross Certificates using the SHA-1 hash algorithm.

CA's MAY continue to use their existing SHA-1 Root Certificates.

Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

S/MIME certificates should continue to be issued with RSA 2048 key sizes with SHA-2 hash algorithm.

7.1.3.1. SubjectPublicKeyInfo

7.1.3.2. Signature AlgorithmIdentifier

7.1.4. Name Forms

Distinguished Names (DNs) should be in the form of X.501 DirectoryStrings.

7.1.4.1. Name Encoding

Refer to CPS for details.

7.1.4.2. Subject Attribute Encoding

Subject attributes should NOT contain only metadata such as '!', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.3. Subscriber Certificate Common Name Attribute

7.1.4.3.1. Subject Distinguished Name Fields

7.1.4.4. Other Subject Attributes

7.1.5. Name Constraints

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

7.1.6. Certificate Policy Object Identifier

7.1.6.1. Reserved Certificate Policy Identifiers

7.1.7. Usage of Policy Constraints Extension

A CA may populate and mark the policy constraints extension as critical.

7.1.8. Policy Qualifiers Syntax and Semantics

A CA may populate the certificatePolicies extension with the OID and policyQualifiers containing the Uniform Resource Locator (URL) of the Visa CPS. A User Notice Qualifier, which points to an applicable RP Agreement, may be used at the discretion of the Issuing CA.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

7.2. CRL Profile

CAs issue X.509 version 2 Certificate Revocation Lists (CRLs) in accordance with the RFC 5280 “Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile”. The CRLs should be published on a repository and/or an Online Certificate Status Protocol (OCSP) responder. The Subscriber and RP software should support the entire base (non-extension) X.509 fields.

The Visa CPS should define the use of extensions supported by the CAs.

7.2.1. Version Number(s)

Refer to CPS for details.

7.2.2. CRL and CRL Entry Extensions

Refer to CPS for details.

7.3. OCSP Profile

OCSP Responses issued by a CA under this policy will conform to the OCSP profile specified in the Internet Engineering Task Force (IETF) RFC 6069 and/or RFC5019.

OCSP responses should either:

- Be signed by the CA that issued the Certificates whose revocation status is being checked, or

- Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. In the latter case, the OCSP signing Certificate should contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560.

Certificate status servers (CSSs) operated under this policy will sign responses using algorithms designated for CRL signing, specified in "Certificate Profile", under the subtitle Algorithm Object Identifiers.

7.3.1. Version Number(s)

The Certificate status servers operated under this policy will use OCSP version 1, specified in the Internet Engineering Task Force (IETF) RFC 2560.

7.3.2. OCSP Extensions

The detailed CRL profiles and use of each extension are specified in "Certificate Profile" and "CRL Profile".

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or Circumstances of Assessment

The CAs are subject to regular compliance audits to confirm that the CA is operating as stated in this CP and in the Visa Certification Practice Statement (CPS). CAs issuing Certificates to external users or replying parties SHOULD undergo WebTrust CA Assessment at least once every three (3) years.

A copy of the compliance audit report SHOULD be submitted to the Visa Cryptographic Review Forum (CRF). The Visa CRF reserves the right to verify that a compliance audit has been performed and that the CA's have complied with the requirements of this CP.

8.2. Identity and Qualifications of Assessor

The compliance auditor should demonstrate competence in the field of Public Key Infrastructure (PKI) and should be thoroughly familiar with the requirements that the CRF imposes on the issuance and management of certificates. The compliance auditor should perform compliance audits as a primary responsibility.

8.3. Assessor's Relationship to Assessed Entity

To prevent any biased outcome, the compliance auditor should not have any financial, legal, or conflicting business relationship with the CA that is being audited.

8.4. Topics Covered by Assessment

The purpose of a compliance audit is to verify that the entity that is subject to the requirements of this Certificate Policy (CP) is acting in accordance with these requirements. The compliance audit covers the requirements that define the operation of a Certificate Authority (CA) under this CP as defined in the Visa CPS.

8.5. Actions Taken as a Result of Deficiency

When a finding is noted, the following actions should be taken:

- The compliance auditor should note the finding as part of the report.
- The compliance auditor should meet with the CA to determine if the finding can be remedied. An action plan should be developed and steps taken to remedy the finding.
- The compliance auditor should report the finding to the Visa CRF.

8.6. Communication of Results

The compliance auditor should provide CA management with a copy of the results of the compliance audit.

8.7. Self-Audits

Visa monitors adherence to its CP, CPS, and these Requirements by performing self-audits on at least a yearly basis. The audits are against a randomly selected sample of the greater of one certificate issued during the period immediately after the previous self-audit sample was taken.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

Imposing fees on a Subscriber or on a Relying Party (RP) is subject to the appropriate authority and policy of the Visa Pricing Committee. Notice of any fee charged to a Subscriber or an RP should be brought to the Pricing Committee's attention.

9.1.1. Certificate Issuance or Renewal Fees

9.1.2. Certificate Access Fees

9.1.3. Revocation or Status Information Access Fees

9.1.4. Fees for Other Services

9.1.5. Refund Policy

9.2. Financial Responsibilities

No stipulation.

9.2.1. Insurance Coverage

9.2.2. Other Assets

9.2.3. Insurance or Warranty Coverage for End-Entities

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 Certificate Authority (CA) or by a Registration Authority (RA) is considered confidential.

This includes, for example, registration and revocation information, logged events, and correspondence between Subscriber and CA. This confidential information should not be disclosed by the CA unless required by law.

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

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

Confidentiality keys may be backed up by the Issuing CA. These keys should be protected in accordance with Chapter 6, TECHNICAL SECURITY CONTROLS. They should not be disclosed without prior consent of the

Subscriber or of a duly authorized representative, such as Visa Human Resources, Legal, and Internal Audit, or as required by law.

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

9.3.2. Information Not Within the Scope of Confidential Information

Certificates, Certificate Revocation Lists (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 is not considered confidential information:

- 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.
- Information that the receiving party lawfully receives free of restriction from a source other than the disclosing party.
- Information that is, or becomes, generally available to the public through no wrongful act or omission on the part of the receiving party.
- 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.
- Information that the disclosing party agrees, in writing, is free of restrictions.

9.3.3. Responsibility to Protect Confidential Information

A CA should ensure that confidential information be either physically and/or logically protected from unauthorized viewing, modification, or deletion. In addition, the CA should ensure that storage media used by the CA system is protected from environmental threats.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

Visa Public Key Infrastructure (PKI) policy is to not disclose private personal information about its Subscribers, customers, employees, and partners without their prior consent, 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 are considered private. This includes, for example, registration and revocation information, logged events, and correspondence between Subscriber and CA. This private information should not be disclosed by the CA or by the 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 should ensure that private personal information be either physically and/or logically protected from unauthorized viewing, modification, or deletion. The CA should also ensure that storage media used by the CA system is protected from environmental threats.

9.4.5. Notice and Consent to Use Private Information

Private personal information will only be used in accordance with applicable law.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Private personal information will only be disclosed if required by law or with prior consent of the individual to which the private personal information applies.

Any request for the disclosure of private information should 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 of any other relevant legislation and applicable organizational policy.

9.4.7. Other Information Disclosure Circumstances

9.5. Intellectual Property Rights

The private key is the sole property of the legitimate holder of the corresponding public key identified in a certificate and it may only be used for the purpose of accessing Visa products and services.

Visa PKIs retain all intellectual property rights in and to the certificates and revocation information that it issued.

Visa retains all intellectual property rights in and to this Visa Certificate Policy (CP).

9.6. Representations and Warranties

A CA issues and revokes certificates, operates its certification and repository services, and provides certificate status information in accordance with this Visa CP.

Authentication and validation procedures are implemented, as described in Chapter 3, IDENTIFICATION AND AUTHENTICATION.

9.6.1. CA Representations and Warranties

CAs should operate in accordance with this Visa CP, the Visa Certification Practice Statement (CPS), and applicable laws when issuing and managing certificates provided to subordinate CAs, RAs, and Subscribers under this Visa CP. See “Compliance with Applicable Law”.

CAs should require that the RAs operating on their behalf should comply with the relevant provisions of this Visa CP regarding the operations of the RAs.

CAs should provide notice of any limitation of liability. See “Indemnities”.

CAs should:

- Issue and administer the Visa CPS that complies with this Visa CP.
- Issue certificates based on requests that are correctly and properly verified, according to “Naming”, if applicable. A CA may delegate this verification, that is, perform due diligence on the certificate requester and certificate request to an RA; however, the CA retains responsibility for ensuring that these functions are performed properly.
- Issue certificates only for use in conjunction with those applications approved by the Visa PKI Team as being appropriate to make use of the PKI.
- Have mechanisms and procedures in place to make subordinate CAs, RAs, and Subscribers aware of and bound to the stipulations in this Visa CP that apply to them.
- Provide a secure environment and proper operations to protect the confidentiality and integrity of the CA.
- Through compliance audit, verify that the operation of the CA complies with this Visa CP. If there are any material changes in the operation of the CA, for example, a change in location or CA platform, the CA should immediately notify the Visa CRF. The CA should verify, through an audit, that the operation of the CA still complies with this Visa CP.
- When publishing or delivering a certificate:
 - Declare that it has issued a certificate to a Subscriber and that the information stated in the certificate was verified in accordance with this Visa CP.
 - Publish the certificate in a repository to which the Subscriber has access or deliver a signed certificate to the Subscriber. This constitutes notice of certification.

- Be individually accountable for actions they perform if the CA personnel are associated with PKI roles. Individually accountable means that there should be evidence that attributes an action to the person performing the action.
- Issuing CAs should take commercially reasonable measures to make Subscribers and RPs aware of their rights and obligations. This applies to the operation and management of any keys, certificates, or hardware and software used in connection with the PKI. Subscribers should also be notified about procedures for dealing with suspected key compromise, certificate or key renewal, and service cancellation.
- Right to Use Domain Name or IP Address: That, at the time of issuance, (i) an implemented procedure described in the CP and/or CPS for verifying that the Applicant either had the right to use or had control of the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) the procedure was followed when issuing the Certificate, and (iii) accurately described the procedure in the Certification Practice Statement(CPS).
- Authorization for Certificate: That, at the time of issuance, an implemented procedure described in the CP and/or CPS for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject, was followed when issuing the Certificate.
- Accuracy of Information: That, at the time of issuance, an implemented procedure described in the CP and/or CPS for verifying the accuracy of the information contained in the Certificate was followed.
- No Misleading Information: That, at the time of issuance, an implemented procedure described in the CP and/or CPS for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading was followed when issuing the Certificate.
- Identity of Applicant: That, if the Certificate contains Subject Identity Information, an implemented procedure described in the CP and/or CPS to verify the identity of the Applicant was followed when issuing the Certificate.
- Subscriber Agreement: That, if the Visa CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a Subscriber Agreement that satisfies these Requirements. If the Visa CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use.
- Status: a 24 x 7 publicly-accessible repository with current information regarding the status (valid or revoked) of unexpired Certificates will be maintained.
- Revocation: That a Certificate will be revoked for any of the reasons specified in these Requirements.

9.6.2. RA Representations and Warranties

A CA should require that its RAs comply with the relevant provisions of this Visa CP and the Visa CPS, as defined in "Registration Authorities".

The RA is responsible for the identification and authentication of Subscribers according to "Initial Identity Validation" and "Certificate Application". Subscribers' rights and obligations, as well as a description of an RP's obligations with respect to use, verification, and validation of certificates are provided by the Visa product or service participation agreement.

An RA may be responsible for revoking certificates in accordance with "Certificate Revocation and Suspension".

RAs are individually accountable for actions performed on behalf of a CA. "Individually accountable" means that there should be evidence that attributes an action to the person performing the action. Records of actions carried out in performance of RAs duties should identify the individual who performed the particular duty. Each Vettor performing RA duties should protect his or her private keys in accordance with Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS, and Chapter 6, TECHNICAL SECURITY CONTROLS. Vettor personnel should undergo an annual compliance validation process.

When an RA submits Subscriber information to a CA, it should 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 Chapter 3, IDENTIFICATION AND AUTHENTICATION and Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.

Submission of the certificate request to the CA should be performed in a secure manner, as described in "Initial Identity Validation".

9.6.3. Subscriber Representations and Warranties

The Subscriber may only use its key pairs and the associated certificates issued under a Visa PKI for the purposes identified in this Visa CP. Key pairs intended for use in a production environment should be generated in that environment in accordance with this Visa CP and Visa CPS. These key pairs should not be cloned, copied, or otherwise conveyed for use in a test or development environment. Key pairs and the associated certificates should not be shared by multiple functional entities. Key pairs generated in a non-production environment should not be used in production implementations of Visa products and/or services.

The Visa CA should obtain an executed version of the Subscriber Agreement prior to issuing the Certificate.

The Subscriber or Terms of Use Agreement should contain provisions imposing the following obligations and warranties (on the Applicant).

- **Accuracy of Information** —An obligation and warranty to provide accurate and complete information to the Visa CA, both in the certificate request and as otherwise requested by the Visa CA in connection with the issuance of the Certificate(s) to be supplied by the Visa CA.
- **Protection of Private Key** —An obligation and warranty by the Applicant to take reasonable measures to maintain sole control of, keep confidential, and properly protect the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) and any associated activation data or device, for example, password or token, in accordance with Chapter 6, TECHNICAL SECURITY CONTROLS.
- **Acceptance of Certificate** —An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy.
- **Use of Certificate** —An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement.
- **Reporting and Revocation** —An obligation and warranty to promptly cease using a Certificate and its associated Private Key and promptly request The Visa CA to revoke the Certificate if:
 - Any information in the Certificate is, or becomes, incorrect or inaccurate.
 - There is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate. Refer to the procedures in "Certificate Revocation and Suspension".
- **Termination of Use of Certificate** —An obligation and warranty to promptly cease use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- **Responsiveness** —An obligation to respond to the Visa CAs instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance** —An acknowledgment and acceptance that the Visa CA is entitled to revoke the certificate immediately if the applicant violates the terms of the Subscriber or Terms of Use Agreement, or if the Visa CA discovers that the Certificate is being used to enable criminal activities, such as phishing attacks, fraud, or the distribution of malware.

9.6.4. Relying Party Representations and Warranties

The RPs should adhere to Visa By-Laws, Operating Regulations, policies, Visa product or service agreements, or operative commercial agreement that relate to specific instances in which an RP trusts or otherwise uses a certificate issued within the Visa PKI. An RP may not act in reliance upon a certificate that has expired, been suspended, revoked, or that includes a revoked certificate in the chain of trust back to the Root CA.

Before using a Subscriber's certificate, an RP should verify that the certificate is appropriate for the intended use.

Before using a certificate, an RP should check the status of the certificate using the relevant CRL, in accordance with the requirements in "Certificate Revocation and Suspension". As part of the verification process, the digital signature on the CRL should also be validated.

9.6.5. Representations and Warranties of Other Participants

9.7. Disclaimers of Warranties

This section is not meant to replace the liability and indemnification provisions of the Visa By-Laws, Operating Regulations, policies, or operative commercial agreement, which should continue to be enforced and in effect.

Nothing in this Visa CP should confer on any third-party authority to act for, bind, create, or assume any obligation or responsibility, or make any representation on behalf of another, except as set forth in this Visa CP. Issuance of certificates in accordance with this Visa CP does not make a CA or an RA, an agent, partner, joint venture, fiduciary, trustee, or other representative of Subscribers or of other RPs. The applicable Subscriber Agreement or Relying Party Agreement defines the relationship between a CA, an RA, and the Subscriber.

9.8. Limitations of Liability

A Visa PKI will not be liable for any damages to Subscribers, RPs, or to any other party arising out of, or related to, the misuse of or reliance on certificates issued by a CA that have been:

- Revoked, suspended, or expired
- Used for unauthorized purposes
- Tampered with
- Compromised
- Subject to misrepresentation, misleading acts, or omissions

Visa does not have Delegated Third-Parties as stated in "PKI Participants".

9.9. Indemnities

The indemnification obligations of Subscribers and RPs are set forth in applicable Subscriber and RPAgreements.

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

- Any false or misleading statement of fact by the Subscriber.
- Any failure by the Subscriber to disclose a material fact, if such omission was made negligently or with the intent to deceive.
- 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.
- 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.

9.9.1. Indemnification by CAs

Any failure on the part of the Subscriber to promptly notify a CA within the Visa PKI of a compromise, disclosure, loss, modification, or unauthorized use of the Subscriber's private key once there has been an actual notification of such an event.

9.9.2. Indemnification by Relying Subscribers

9.9.3. Indemnification by Relying Parties

9.10. Term and Termination

9.10.1. Term

This Visa CP remains in force until a notice is communicated by Visa CRF on its website at <https://visawiki.trusted.visa.com/spaces/APC/pages/2141831305/PKI>.

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

The conditions and effects resulting from termination of this document will be communicated by Visa CRF on its website at <https://visawiki.trusted.visa.com/spaces/APC/pages/2141831305/PKI> and will outline the provisions that may survive its termination and remain in force.

9.11. Individual Notices and Communications with Participants

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

9.12. Amendments

The Visa CRF is the responsible authority for reviewing and approving changes to the Visa CP. Written and signed comments on proposed changes should be directed to the Visa CRF Chairman as described in "Contact Person". Decisions about proposed changes are at the sole discretion of the Visa CRF.

9.12.1. Procedure for Amendment

The PKI may provide notification, in writing, of any proposed changes to this Visa CP following approval by the CRF. The notification will contain a statement of proposed changes and the final date that comments can be submitted.

Written and signed comments on proposed changes should be directed to the Chairman of the Visa CRF, as described in "Contact Person". Decisions about proposed changes are at the sole discretion of the Visa CRF.

9.12.2. Notification Mechanism and Period

9.12.3. Circumstances under which OID must be Changed

Changes to Object Identifiers (OIDs) are at the discretion of the Visa CRF.

9.13. Dispute Resolution Provisions

Refer to Visa Operating Regulations and Visa By-Laws or to the Operative Commercial Agreement.

9.14. Governing Law

Refer to Visa Operating Regulations and Visa By-Laws or to the Operative Commercial Agreement.

9.15. Compliance with Applicable Law

Refer to Visa Operating Regulations and Visa By-Laws or to the Operative Commercial Agreement.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

Refer to Visa Operating Regulations and Visa By-Laws or to the Operative Commercial Agreement.

9.16.2. Assignment

Refer to Visa Operating Regulations and Visa By-Laws or to the Operative Commercial Agreement.

9.16.3. Severability

Refer to Visa Operating Regulations and Visa By-Laws or to the Operative Commercial Agreement.

9.16.4. Enforcement

Refer to Visa Operating Regulations and Visa By-Laws or to the Operative Commercial Agreement.

9.16.5. Force Majeure

A Visa PKI is not to be held responsible for any delay or failure in performance of its obligations if such delay or failure is caused by fire, flood, strike, civil, governmental, or military authority, acts of terrorism or war, an 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 of its subcontractors.

9.17. Other Provisions