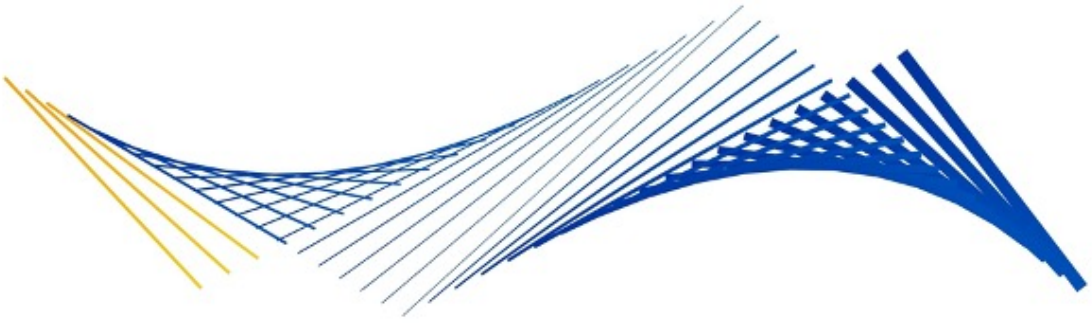
Visa Public Key Infrastructure Certification Practice Statement (CPS) For Internal Trust

Version 1.2

Visa PKI

March 16, 2026



Contents

Important Note on Confidentiality and Copyright

About This Guide

Visa Certification Practice Statement (CPS) 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

This Certification Practice Statement (CPS) defines the practices and procedures for the following Visa Public Key Infrastructures (PKIs). These PKIs issue digital certificates in support of strong authentication.

- 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
- VSDC Certificate Authority

This CPS is in conformance with the Visa Certificate Policy (CP).

Visa has implemented a PKI for issuing and distributing digital certificates to support Visa products and services. This infrastructure is known as the Visa PKI and includes a hierarchy of entities called Certificate Authorities (CAs).

These CAs are trusted third parties that issue End-Entity Transport Layer Security (TLS) and Internet Protocol Security/ Virtual Private Network (IPsec/VPN) certificates to Visa clients, Visa employees, and Visa devices or Visa Smart Debit/Credit (VSDC) certificates for Visa issuers.

At the top of the PKI hierarchy are the following Root Certificate Authorities (CAs):

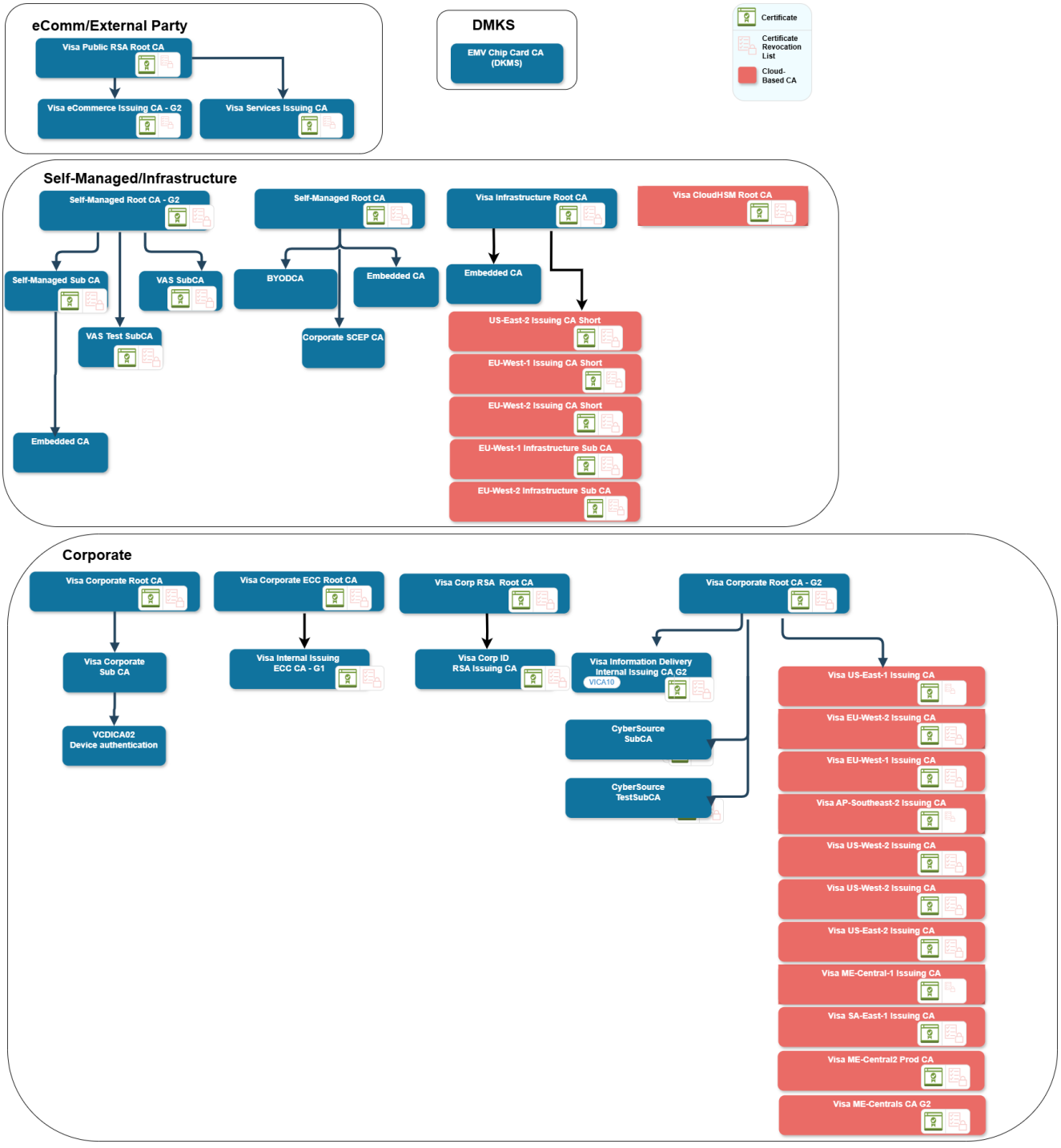
- Visa Public RSA Root CA
- Visa Corporate Root CA
- Visa Corporate Root CA G2
- Visa Corp RSA Root CA
- Visa Self Managed Root CA
- Visa Self Managed Root CA G2
- Visa Infrastructure Root CA
- Visa Corporate ECC Root CA
- Visa CloudHSM Root CA

The CAs are organized in hierarchies as follows:

- **Root Certificate Authorities (CAs)** are at the top of the hierarchy.
- **Intermediate Certificate Authorities (CAs)** are directly subordinate to the Root CAs, which have subordinate Issuing CAs.
- **Issuing Certificate Authorities (CAs)** are the lowest level of the hierarchy and only issue End-Entity certificates. They are subordinate to the Intermediate CAs and Root CAs.

The following figure illustrates the PKI hierarchies.

Figure 1–1: PKI Hierarchies



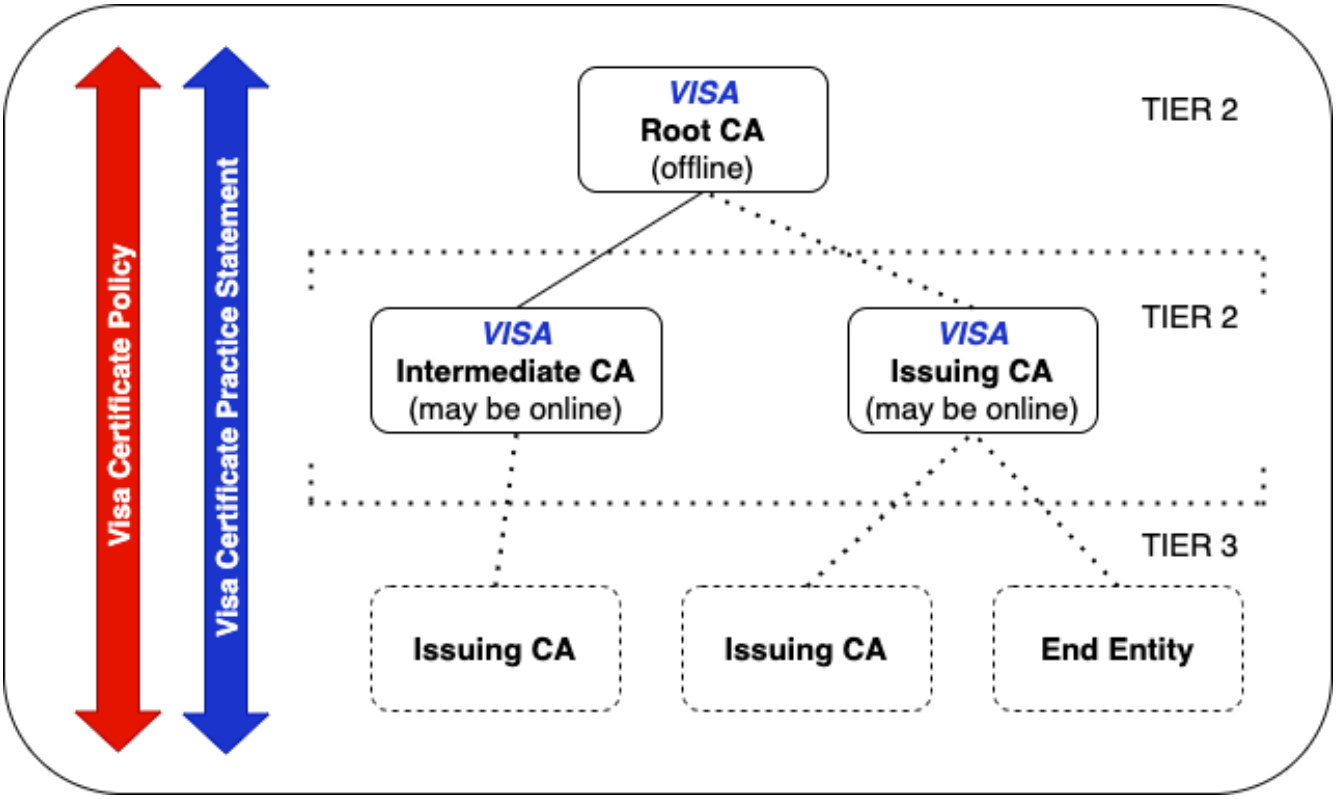
Cross-certification between external CAs and CAs is not supported. The Visa PKI hierarchy is a closed PKI.

The PKI CP describes the legal, business and technical requirements for issuing, revoking, renewing, and distributing digital certificates to support Visa products and services. This CPS describes how these requirements are met in issuing Visa certificates to Subscribers.

The PKI is used specifically to issue Visa TLS Client, Visa TLS Server, Visa TLS Server and Client, and Visa Smart Debit/Credit (VSDC) certificates to Visa issuers.

The following figure illustrates the Visa Document Structure.

Figure 1–2: Visa Document Structure



The CP is the overall certificate policy document related to the PKI. As shown in Figure 1-2, the CP (red spanning arrow) encompasses policy for the entire PKI. This CP is specific to the functioning of CAs within the hierarchy. Other documents including Key Ceremony scripts and Business Recovery Plans (BRPs) supplement this CPS.

The CAs operate in a closed environment. Certificates can only be issued to entities that have a contractual agreement with Visa or Visa Business Groups and clients, and are bound to comply with Visa Operating Regulations and policies or with an Operative Commercial Agreement.

This CPS does not have details about the operations of the PKI; rather it provides an overview of the practices. Details of the operations are found in supporting documents.

1.2. Document Name and Identification

This CPS is titled Visa Public Key Infrastructure (PKI), Certification Practice Statement (CPS).

The object identifiers (OIDs) used for certificates issued under this CPS 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
1.1	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

This PKI will sign and issue Transport Layer Security (TLS) Client certificates, Server certificates, Server and Client certificates, to web browsers, web servers, application servers, and network devices that have a contractual agreement with Visa or Visa region clients.

Visa does not have delegated third-parties.

1.3.1. Certification Authorities

A Certificate Authority (CA) operating under the PKI will sign certificates that bind Subscribers to their private keys. The CAs are responsible for:

- The creation and signing of certificates binding Subscribers, PKI administrators, and Vettors with their signature verification keys
- Promulgating certificate status through publishing certificates and Certificate Revocation List (CRL) status to publicly available repositories
- Adherence to this CPS and the CP

1.3.2. Registration Authorities

There is at least one Registration Authority (RA) supporting each CA. The RAs operating within a CA service perform identification and authentication in the verification of certificate request content.

The primary responsibility of the RA is to verify that the party submitting the certificate request is who it claims to be and is authorized to submit the request on behalf of the certificate request originator, has a valid business relationship with Visa, and verifies that the certificate has been transferred from the originator to the RA in a secure manner.

The RA is tasked to verify certificate revocation requests in a similar manner; that is, verifying the party submitting the revocation is who it claims to be and is authorized to submit the revocation request on behalf of the originator.

RA administrators are employees of Visa, Visa subsidiaries, or Visa clients and have a valid business relationship with Visa, and are contractually bound to comply with Visa By-Laws, Operating Regulations, policies, or operative commercial agreement.

Enrollment Initiation

1.3.3. Subscribers

For the purpose of this CPS, a Subscriber is an entity such as a person, device, or application that is a holder of a private key corresponding to a public key that has been issued a Transport Layer Security (TLS), Client certificate, Secure Server certificate, Server and Client certificate, or a Visa Smart Debit/Credit (VSDC) certificate by a CA. For a device or an application, a person authorized by the organization owning the device or application is referred to as the Subscriber. Responsibility and accountability for each certificate is attributable to an identified entity.

Eligibility for a certificate is determined by the relevant Visa product and/or service.

1.3.4. Relying Parties

A Relying Party (RP) is an entity or person that relies on a certificate or information about the certificate that is issued by a CA. RPs are contractually bound to comply with Visa By-Laws, Operating Regulations, policies, or operative commercial agreement.

1.3.5. Other Participants

1.4. Certificate Usage

This CPS is applicable to certificates issued and distributed by a CA. The practices described in this CPS apply to the issuance, use, suspension, or revocation of Subscribers of the PKI.

1.4.1. Appropriate Certificate Uses

Certificates issued under this CPS are suitable for:

- Protecting the integrity and authenticity of business transactions
- Protecting the confidentiality of information to facilitate the confidential transfer and restrict access to that information

1.4.2. Prohibited Certificate Uses

Certificates issued under this CPS are prohibited from being used for any other purpose.

1.5. Policy Administration

1.5.1. Organization Administering the Document

The Visa Cryptographic Review Forum (CRF) is the overall administrative authority of this CPS. It is the responsible authority for reviewing and administering changes to this CPS.

Written and signed comments on proposed changes should be directed to the Chairman of the CRF as described below.

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

The Visa CRF is the administrative entity for determining CPS suitability for 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 should 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 Public Key Infrastructure (PKI) such as key component, Certificate Authority (CA) system, or Certificate Authority (CA) facility.

Activation Data: Data (other than the keys themselves) that is used and needed to activate a private key. Examples include a Personal Identification Number (PIN), password, or 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 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 are 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 Certificate Authority certificate that signed it, and all of the Certificate Authority certificates up to the Root Certificate Authority.

Certificate Authority: An authority trusted by one or more users to issue and manage X.509 certificates and Certificate Revocation Lists (CRLs). CAs have certificates that allow them to sign other certificates and/or CRLs. Within the Visa Public Key Infrastructure (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 Certificate Policy (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: A statement of the practices that a CA uses in issuing certificates. The statement is a comprehensive description of details such 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. This CPS illustrates how the CA satisfies the requirements included in the Certificate Policy (CP) that governs it.

Certificate Revocation List: 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 Certificate Revocation List (CRL) issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked serial numbers of the certificates, and the specific times and reasons for revocation. CRLs are used to check the status of certificates. They may be published in a repository or through an Online Certificate Status Protocol (OCSP) responder.

Certificate Systems: The system used by a CA or delegated third-party to provide identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Confidential: A security classification used to describe information which, if disclosed, could result in personal loss or minor financial loss. Personal information and tactical information is considered confidential.

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

Cross-Certification: The process that describes 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 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 so 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)
- User ID
- Domain component (dc)

Dual Control: A process using two or more separate entities (usually persons), operating in concert to protect sensitive functions or information so no single entity is able to access or utilize 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, a client, for example, cardholders, merchants, and employees
- Organizations, that is, Visa Business Groups, clients or their agents or merchants
- Devices or applications (for example, servers and client software) 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 certificates 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 was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian Government's Communication Security Establishment (CSE), and may be adopted by the financial community through the American National Standards Institute (ANSI). The different levels (1 to 4) within the standard provide different levels of security and in the higher levels, have different documentation requirements.

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, whether maliciously or accidentally.

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

Key: When used in the context of cryptography, it is a value (which may be secret) and a sequence of characters that is used to encrypt and decrypt data. A key is a uniquely 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. 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, service, or activity occurrence.

Online Certificate Status Protocol: An online protocol developed by the Internet Engineering Task Force (IETF) (Request for Comment [RFC] 6960) to allow a Relying Party to obtain more timely information regarding the revocation status of a certificate than is possible with Certificate Revocation Lists (CRLs).

Object Identifier: The unique alphanumeric identifier registered under the International Organization for Standardization (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 (CA): A 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: A standard that provides recommendations for the implementation of public-key cryptography based on the Rivest, Shamir, Adelman (RSA) algorithm, covering the following aspects: cryptographic primitives; encryption schemes; signature schemes, and so on.

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 to develop Internet standards needed to support an X.509-based Public Key Infrastructure (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: People, generally employees, associated with the operation, administration, and management of a CA or RA.

Policy: A set of laws, rules, and practices that regulate 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: A 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, and technology, audit, and control mechanisms used to manage 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. 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 (RDN): 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 should be in different bases or branches, of the directory. An example of a DN is cn=Road Runner, ou=bird, on=mammal, c=US.

RDNs would be:

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

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

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. Relying Parties (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 Agreement is entered into by a party wishing to rely on a certificate and the information contained in it. A Relying Party Agreement governs the terms and conditions under which the 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 on which the RP wishes to rely. For Visa products and services, Relying Party 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 technology where data is stored logically. In PKI terms, a repository accepts certificates and Certificate Revocation Lists (CRLs) from one or more CAs and makes them available to entities that need them to implement 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 certificate revocation list (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 so 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 personal harm or death. This is equivalent to the Visa Secret classification.

Signature Verification Certificate: Often referred to as a Signature Certificate. It is the certificate that contains 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 Certificate Revocation Lists (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 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: A certificate used to verify the authentication of an End-Entity to a server when a connection is being established through a Transport Layer Security (TLS) session (secure channel).

TLS Server Certificate: A 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 Transport Layer Security (TLS) session (secure channel).

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

User Notice Qualifier: A User Notice Qualifier in an X.509 certificate is intended for display to a 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. Unicode Transformation Format (8-bit) (UTF-8) is a multibyte 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 31 December, 2003, all certificates were required to use UTF8String encoding for subject names.

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

Visa Certificate Authority: This is comprised of the Root Certificate Authority (CA) and the Issuing Certificate Authorities (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
- Certificate Authorities, that is Regional Business Units or clients only

Visa Public Key Infrastructure or Visa PKI: This is an X.509 PKI implemented by Visa for issuing and managing digital certificates to be used in conjunction with Visa products and services. This PKI consists of a hierarchy of entities called 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 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 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 which has a service agreement with Visa
CP	Certificate Policy
CPS	Certification Practice Statement
CRF	Cryptographic Review Forum
CRL	Certificate Revocation List
DN	Distinguished Name
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
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
OCSP	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
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

Acronym	Spelled Out Form
SHA	Secure Hash Algorithm
Smart Card	Electronic identity and authorization card used by Information Delivery Vettors 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 Standards and Technology (NIST) Special Publication SP800-88 Rev-2
- Internet Engineering Task Force (IETF) Public Key Infrastructure Extension (PKIX) Internet X.509 Public Key Infrastructure Certificate Policy (CP) and CPS Framework (also known as Request for Comment (RFC) 3647)
- Federal Information Processing Standard (FIPS) Publication (PUB) 140-2 and 140-3
- International Standards Organization (ISO) 9564-1 and International Standards Organization (ISO) 11568-5
- Public Key Cryptography Standard (PKCS) #7
- Internet Engineering Task Force (IETF) Public Key Infrastructure Extensions (PKIX) Certificate and Certificate Revocation List (CRL) Profile, as defined in Request for Comment (RFC) 5280
- Secure Hash Algorithm (SHA-1, SHA-2) algorithm in accordance with Federal Information Processing Standard (FIPS) Publication (PUB) 180-4 2012
- Internet Protocol Security/ Virtual Private Network (IPsec/VPN)
- 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:
Italics	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 *not applicable*. 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 CP is 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 CRF, as described in Chapter 1, INTRODUCTION.

Each Certificate Authority (CA) has one repository of record that holds certificates and Certificate Revocation Lists (CRLs) within the Certificate Authority's (CAs) database.

Certificate revocation information from CRLs is published by the appropriate Certificate Authority (CA) in accordance with the requirements of "Certificate Revocation and Suspension" and "Key Escrow and Recovery".

Visa provides Online Certificate Status Protocol (OCSP) services as described within this CPS.

2.2. Publication of Information

Subscribers are notified that a Certificate Authority (CA) publishes information submitted by them to publicly accessible directories in association with certificate status information. The publication of this information should be within the limits of "Privacy of Personal Information" and "Intellectual Property Rights". The Certificate, Online Certificate Status Protocol (OCSP) responders, and Certificate Revocation List (CRL) publication should be in accordance with the various sections in Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.

A Certificate Authority (CA) reserves the right to make available and publish information about its operations consistent with the Visa Certificate Policy (CP). A Certificate Authority (CA) may refrain from making publicly available certain subcomponents and elements of documents, such as certain security controls, procedures related with the Certificate Authority (CA), RA, and any other components of the environment.

Certificate Authorities (CAs) should provide full text version of this Certification Practice Statement (CPS) when necessary for the purposes of audit or as required by law.

2.3. Time or Frequency of Publication

Visa reviews and updates the CPS as necessary to incorporate required compliance changes. Any changes to the CPS should be submitted to the CRF for approval as defined in "Policy Administration".

Certificate information should be distributed and/or published promptly upon issuance. Maximum time limits and frequency of certificate and CRL publishing are described in Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS of this CPS.

2.4. Access Controls on Repositories

Certificate Authorities (CAs) may keep access to its public repository available to RPs in order to validate the certificates it has issued. Certificate Authorities (CAs) may limit or restrict access to its services such as the publication of status information on external databases and private directories.

Certificate Authorities (CAs) should include within its End-Entity certificates the Uniform Resource Locator (URL) of the website where the CRL is published.

3. IDENTIFICATION AND AUTHENTICATION

This chapter describes the requirements for authentication of the certificate requester. In cases where the certificate requester is not the Subscriber, it also describes the requirements for establishing that the certificate requester is authorized to submit the request on behalf of the Subscriber.

In all cases, the certificate request should be submitted by an individual either on his own behalf or on the behalf of an application, server, or device that will use the certificate.

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 should not be blank and should use printable characters, for example X.501 printableString, IA5String, or Unicode Transformation Format (UTF8) name.

Subscribers may use an alternative name in the Subject Alternative Name (SAN) extension field.

The Subject names in a Certificate Authority (CA) issued certificate should comply with the X.500 Distinguished Name (DN) form.

Distinguished Names (DN) Restrictions

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

Subscribers should not use fictitious names.

Certificates that contain wildcard characters ("wildcard certificates") may be signed with the following restrictions:

- 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).
- No more than 100 servers or containers should use a single wildcard certificate.

Server certificates that contain a domain name not owned by Visa ("foreign entity certificates"), for example, server_name.BankX.com, may be signed and require the following:

- 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

The method to prove possession of a private key should be Public Key Certificate Standard (PKCS) #10 or another cryptographically equivalent format such as a self-signed EMVCo Certificate Request.

3.2.2. Authentication of Organization and Domain Identity

A person authorized to act on behalf of an organization can make an application for the organization to become a Subscriber. The certificate application should include information about that server/device, in a form Certificate Signing Request (CSR), as requested by the relevant Visa Certificate Authority (CA). The application should be provided in a secure manner, that is, secure website, Secure Multipurpose Internet Mail Extension (S/MIME), or equivalent method approved by the relevant Certificate Authority (CA), or through a separate written document appropriately marked as Confidential.

The Registration Authority (RA) handling a request should rely on an existing business process and comply with the requirements set forth in the *Visa Global PKI - Vettor Operations Guide*.

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

For an application to acquire a Transport Layer Security (TLS) Client certificate should be made by an authorized person. Each Business Group is responsible for defining its vetting process and enforcing its procedures.

A hard copy or electronic copy of the information should be maintained by a RA for audit purposes for a period of ninety (90) days.

A request to acquire a Vettor certificate can be made only by designated Visa employees or authorized contractors. Their manager is responsible for vetting their credentials and verifying a background check was completed. The Business Group RA manager or senior manager should notify Certificate Authority (CA) administrators by secure email: PKIPolicy@visa.com that a Vettor's certificate should be issued to the designated individual. The request should be manually vetted by the appropriate Certificate Authority (CA) administrators.

A request to acquire a Certificate Authority (CA) or RA administrator certificate can be made only by designated Visa employees after they complete the appropriate forms and follow the established processes and procedures. Their management is responsible for vetting their credentials and verifying a background check was completed. The Visa Public Key Infrastructure (PKI) Facility Manager or their delegate should notify a Certificate Authority (CA) administrator that an administrator's certificate should be issued to the designated individual. The request should be manually vetted by the appropriate Certificate Authority (CA) administrators.

The Subscriber is responsible for:

- Generating a request that meets PKI requirements as stated in this Visa CPS
- 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 Vettor or Certificate Authority (CA) administrator is responsible, on behalf of a Certificate Authority (CA) for:

- Completing the verification and authorization requirements as stated in, *Visa Global PKI - Vettor Operations Guide*.

3.2.4. Non-Verified Subscriber Information

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

3.2.5. Validation of Authority

Authorization to request a certificate will be required to be an official appointment of such (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

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

3.2.6. Criteria for Interoperation or Certification

Cross-certification between external Certificate Authorities (CAs) and Visa Certificate Authorities (CAs) is not supported. The Visa PKI hierarchy is a closed PKI.

3.3. Identification and Authentication for Re-Key Requests

The re-key of End-Entity certificates is not supported.

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 Request

Certificate Authorities (CAs) or RAs authenticate a request for revocation of a certificate in the same way as they submit a certificate request. Certificate Authorities (CAs) or RAs should keep a record of the type and details of the revocation request including the identity and authentication of the requesting person for at least ninety (90) days.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

The procedures and requirements with respect to an application for a certificate are set out in this Certification Practice Statement (CPS) and have Business Group's specific components. An application for a certificate does not obligate the Certificate Authority (CA) Vettor to issue a certificate.

Application for End-Entity Certificate

The certificate application should follow the requirements described in "Initial Identity Validation", as well as fulfill the requirements of any applicable agreement.

Each application should be accompanied by:

- Proof of authorization for any requested certificate attributes if other than those allowed for the type of certificate being requested, such as Subject Alternate Names (SANs) and other extended key usages
- A properly formatted Public Key Certificate Standard (PKCS) #10 certificate request or equivalent

Application for Certificate Authority (CA) and Registration Authority (RA) administrators and Vettor certificates should follow the requirements listed in "Procedural Controls".

Required Information for a Certificate Request

Any Subscriber information should be complete, validated, and accurate with full disclosure of all required information in connection with a certificate request. The Subscriber information should be validated by one of the following:

- Registration Authority (RA) Manager(s)
- Vettors
- Certificate Authority (CA) Administrators

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 documentation; prior to certificate issuance.

4.1.1. Who Can Submit a Certificate Application

Below is a list of roles authorized to submit certificate applications:

- An authorized representative of an Organization or entity that have 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 an RA

4.1.2. Enrollment Process and Responsibilities

All end-user Certificate Subscribers consent to the Subscriber Agreement and complete the enrollment process consisting of:

- Completing the Certificate Application form and providing 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 certificate authorities.
- 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

A Certificate Authority (CA) or RA should perform identification and authentication procedures to validate a certificate request. Vettors should perform identification and authentication of required Subscriber information as stated in "Initial Identity Validation".

The CA MAY use the documents and data provided in Section 3.2 to verify certificate information, provided that the CA obtained the data or document from a source specified under Section 3.2 no more than 825 days prior to issuing the Certificate.

4.2.2. Approval or Rejection of Certificate Applications

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

4.2.3. Time to Process Certificate Applications

The period of time between receiving a valid request for a certificate, the validation and the issuance and publishing of a certificate should be within the defined Service Level Agreements (SLA) for the relevant Certificate Authority (CA).

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

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.

4.4.2. Publication of the Certificate by the CA

A Certificate Authority (CA) is responsible for repository and publication functions. A Certificate Authority (CA) should publish certificates in a repository based on the certificate publishing practices defined in this Visa CPS or for VSDC make certificate information available as necessary through ad hoc reporting.

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 Certificate Authority (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 Certificate Authority (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 Certificate Authority (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 a RA for authentication in order to operate the RA applications should not be used for any other purpose.

The Subscriber can only use production certificates issued by an Issuing Certificate Authority (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 Certificate Authority (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 certificate private keys should be stored in a tamper resistant security module (for example, a 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.

Email Encryption and Signing Certificate and Usage

An email encryption certificate is a certificate with email encryption extensions. An email signing certificate is a certificate with email signing extensions. Only the Visa Corp ID RSA Issuing CA should sign email encryption and signing certificates and only for Visa Internal use. Individual email encryption and signing certificates private keys should be stored within Visa Approved Secure Storage.

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 Certificate Renewal

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

No Stipulation.

4.8.2. Who May Request Certificate Modification

No Stipulation.

4.8.3. Processing Certificate Modification Requests

No Stipulation.

4.8.4. Notification of New Certificate Issuance to Subscriber

No Stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

No Stipulation.

4.8.6. Publication of the Modified Certificate by the CA

No Stipulation.

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

No Stipulation.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

A certificate 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

The CA should revoke a Certificate if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate without specifying a CRLreason (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
3. The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate is Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6 (CRLReason #1, keyCompromise);
4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate, including but not limited to those identified in Section 6.1.1.3 (CRLReason #1, keyCompromise);
5. The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
6. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
7. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation);
8. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
9. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
10. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement (CRLReason #4, superseded);
11. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading (CRLReason #9, privilegeWithdrawn);
12. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate (CRLReason #9, privilegeWithdrawn);
13. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason #9, privilegeWithdrawn);
14. The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate (CRLReason #1, keyCompromise);

15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
16. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (CRLReason #9, privilegeWithdrawn);
17. When a Subscriber fails to comply with obligations set out in this Visa CP or in the Visa CPS (CRLReason #9, privilegeWithdrawn);
18. When the basis for any information in the certificate changes (CRLReason #9, privilegeWithdrawn);
19. When the business relationship under which the certificate was issued changes (CRLReason #9, privilege-Withdrawn);
20. When a Subscriber is no longer participating in the Visa product or service for which the certificate was issued (CRLReason #9, privilegeWithdrawn);
21. Upon suspected or known compromise of the private key or of the media holding the key (CRLReason #1, keyCompromise);
22. Upon notification of termination of an employee or Subscriber (CRLReason #9, privilegeWithdrawn);
23. When the certificate has been issued to an ineligible Subscriber (CRLReason #9, privilegeWithdrawn);
24. When a Subscriber no longer needs access to Visa products or services (CRLReason #9, privilegeWithdrawn);

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this CP or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.2. Who Can Request Revocation

The revocation of a certificate may 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 supervisor or manager on behalf of a Subscriber.
- An RA associated with the Issuing Certificate Authority (CA).
- The Issuing Certificate Authority (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). 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]https://visawiki.trusted.visa.com/spaces/APC/pages/2

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.

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 Certificate Authority (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 CA Must Process the Revocation Request

The CA should **begin investigation** of a TLS Certificate Problem or a certificate revocation request within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least one of the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that they didn't receive the goods they ordered); and
4. Relevant legislation.

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

Certificate Authorities (CAs) synchronizes their CRL issuance and publishing with a web server to ensure the most recent CRL is available to RPs.

It is the Relying Party's responsibility to check the status of all certificates in the certificate validation chain against current Certificate Revocation Lists (CRLs) or OCSP responder, prior to their use, including the authenticity and integrity of CRLs or OCSP responder. If the RP caches the CRL, it should retrieve a 'fresh' CRL at least once a day.

CRLs are available on the Uniform Resource Locators (URLs): https://enroll.visaca.com/.

OCSP responders are available on the Uniform Resource Locators (URLs): https://ocsp.visa.com/ocsp

The CRL distribution points are identified in every certificate.

4.9.7. CRL Issuance Frequency

A Certificate Authority (CA) should issue an up-to-date CRL to attest the most current certificate status of all issued certificates. Online active issuing Certificate Authorities (CAs) issue a current CRL at least once every 24 hours. In cases where a Subscriber certificate is revoked, the Certificate Authority (CA) will issue a new CRL.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. Online Revocation/Status Checking Availability

OCSP responses should conform to RFC6960 and/or RFC5019. OCSP responses should either:

1. be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. be signed by an OCSP Responder which complies with the OCSP Responder CertificateProfile in Section 7.1.2.8.

OCSP responses for Subscriber Certificates should have a validity interval greater than or equal to eight hours and less than or equal to ten days.

4.9.10. On-Line 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 will make reasonable efforts to notify potential Relying Parties if it discovers, or has reason to believe 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 in Section 4.9.1 are suspected or known. A Certificate Authority (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 may 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 supervisor or manager on behalf of a Subscriber.
- An RA associated with the Issuing Certificate Authority (CA).

4.9.15. Procedure for Suspension Request

The procedures and requirements with respect to the suspension of a certificate are the same as those for revocation described in Section 4.9.1 through Section 4.9.6.

4.9.16. Limits on Suspension Period

If a certificate is suspended pending verification of a revocation request, the suspension period should be appropriate to the period needed to validate the revocation request.

At the end of the suspension period, the Certificate Authority (CA) should make a determination regarding whether the certificate will be reinstated, the suspension period extended, or the certificate revoked.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder as stated 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 conditions.

4.10.3. Optional Features

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

4.11. End of Subscription

A Subscriber's subscription service ends if its certificate expires or is revoked or if the business relationship with Visa expires or is terminated.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

Certificate Authority (CA) private keys 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 key recovery for email encryption may be recovered by documented processes.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

5.1. Physical Security Controls

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

5.1.1. Site Location and Construction

The following requirements and procedures should be implemented:

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

5.1.2. Physical Access

1. Visa Public Key Infrastructure (PKI) Certificate Authorities (CAs) should reside in a physically secure environment not used for any business activities unrelated to the management of cryptographic services.
2. To support the objective of protecting against intrusions, the physically secure environment should include a:
   - Data center and/or room with true floor to ceiling walls (slab-to-slab walls)
   - Cage and/or room with locking mechanisms requiring two-person access
   - Use of Host Security Module (HSM) for key protection where possible
   - Storage of smart cards in a safe or other secure manner
3. One or more surveillance cameras should provide continuous monitoring of entry and exit to the physically secure environment. Activation of the recording function should either be continuous or done through a motion detector, which is separate from the intrusion detection system. Continuous lighting should be available for the cameras.
4. Surveillance cameras should monitor activities within the physically secure facility. Under no circumstances can surveillance cameras be configured to allow the monitoring of computer screens, keyboards, or Personal Identification Number (PIN) pads.
5. The physically secure environment should have an intrusion detection system:
   - The intrusion detection system should have 24-hour monitoring.
   - The system should be capable of recording and archiving alarm activity.
   - Alarm activity includes unauthorized entry attempts or any deliberate or inadvertent actions that disable the intrusion detection system.
   - All logged alarm activity information should be reviewed and resolved.
   - Documentation of the review and resolution should be retained for ninety (9) days.
6. Entrance and exit should require at least the use of individual access proximity cards in conjunction with biometric, requiring at least two authorized individuals, to access the Certificate Authority (CA) physical environment.

7. Physical keys and combination locks can only be used as a secondary access control mechanism:
    - Physical room and bypass keys to locks should be marked so that each individual key can be identified, controlled and accounted for.
    - The distribution and collection of keys should be recorded. A record of individual access for each key should be maintained.
8. When a Personal Identification Number (PIN) or password is recorded, it should be stored in a security container accessible only to authorized personnel.
9. The access control systems should:
    - Be inspected at least quarterly by qualified personnel.
    - The inspection documentation should be retained for at least ninety (90) days period to support audit requirements.
10. Physical access to the secure environment containing certificate authority related systems and to the actual secure cryptographic devices(s) should be limited to authorized individuals and a minimum of two-person control. This practice is referred to as split knowledge and dual control1.
11. At least two authorized individuals should be present within the physically secure environment. The presence of a single individual for more than 60 seconds will cause an alarm event, the resolution of which should be reviewed and resolved.
12. The door for entrance should not release if the second individual does not complete his authentication within 60 seconds of the first individual. This will cause the system to reset and require the restart of the entry process.
13. Personnel with access to the physically secure environment should not have access to the recorded images. Recorded images should be securely retained for at least ninety (90) days.
14. Visitors (contractors, maintenance personnel, and so on) requiring access to the physically secure environments should be escorted by authorized individuals and sign an access logbook. This log should be maintained within the physically secure facility. This logbook has to include:
    - Date and time in/out
    - Name and signature of visitor
    - Participant's organization or affiliation of visitor
    - Reason for visit or a ticket number

Certificate Authority (CA) Physical Security Logs

- Logs of access should be reviewed on a periodic basis and the review should be documented.
- Access granting, revocation, and review procedures should be documented.
- Alarm events are recorded and should be documented by the facility security function, and reported to the secure room manager.
- The use of any emergency entry or exit mechanism should cause an alarm event.
- A process should exist for synchronizing the time and date stamps of the access, intrusion detection and monitoring (camera) systems to ensure accuracy of logs. Documentation of the synchronization should be retained for at least ninety (90) days.

5.1.3. Power and Air Conditioning

Certificate Authority (CA) facility management should ensure that the power, air conditioning, water exposures, fire prevention and protection, and other environmental controls are sufficient to support the operation of the Certificate Authority (CA) system.

5.1.4. Water Exposure

Certificate Authority (CA) facility management should ensure that the power, air conditioning, water exposures, fire prevention and protection, and other environmental controls are sufficient to support the operation of the Certificate Authority (CA) system.

5.1.5. Fire Prevention and Protection

Certificate Authority (CA) facility management should ensure that the power, air conditioning, water exposures, fire prevention and protection, and other environmental controls are sufficient to support the operation of the Certificate Authority (CA) system.

5.1.6. Media Storage

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

5.1.7. Waste Disposal

The PKI should ensure the destruction or sanitization of all confidential media so that the information on the media can no longer be recovered, prior to release for disposal.

5.1.8. Off-site Backup

The PKI Certificate Authorities (CAs) should ensure that facilities used for off-site backup have the same level of security as the primary Certificate Authority (CA) site.

5.2. Procedural Controls

5.2.1. Trusted Roles

A Certificate Authority (CA) requires the separation of critical CA functions. The CA personnel should perform the following functions with separate knowledge and dual control:

- Generation of a new CA key pair.
- Replacement or renewal of a CA key pair.
- Change in the certificate profile security policy as approved by the Visa Change Management Process.

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 systems.
  - 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 (RA) Trusted Roles

The Visa Cryptographic Review Forum (CRF) requires that the Registration Authority (RA) personnel understand their responsibility for the identification and authentication of prospective Subscribers and 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 Subscriber's information to the issuing Certificate Authority (CA).
- Provision of shared secrets, as required, for authenticating Subscribers.
- RA agents (Vettors) issuing TLS (except S/MIME) certificates should undergo annual compliance to firm their knowledge and responsibilities.

5.2.2. Number of Individuals Required per Task

The Visa Public Key Infrastructure (PKI) should implement the principle of split-knowledge and dual control for the following tasks:

- Signing of a root, intermediate or issuing Certificate Authority (CA) certificate.
- Change in the certificate profile security policy as approved by the Visa Change Management Process.

The Visa Public Key Infrastructure (PKI) should have a verification process that provides an oversight of activities performed by privileged Certificate Authority (CA) role-holders.

The activities include issuing certificates, generating keys, and administering the Certificate Authority (CA) configuration settings.

5.2.3. Identification and Authentication for Trusted Roles

Certificate Authority (CA) personnel involved in the operation of a Certificate Authority (CA) should have their identity and authorization verified before they are:

1. Included on the access list for the Certificate Authority (CA) facility
2. Included on the access list for physical access to the PKI system
3. Given appropriate credentials for the performance of their Certificate Authority (CA) operation's role and these credentials should:
   - Be directly attributable to an individual.
   - Not be shared.
   - Be restricted to actions authorized for that role through the use of a combination of Certificate Authority (CA) software, operating system, and procedural controls.

Certificate Authority (CA) operations should be secured using token-based strong authentication and encryption (that is, smart cards).

5.2.4. Roles Requiring Separation of Duties

5.3. Personnel Controls

The PKI requires that personnel performing duties with respect to the operation of a Certificate Authority (CA) or who are stakeholders in the management of a Certificate Authority (CA) should:

- Be appointed in writing.
- Be bound by the terms and conditions of the role they are to perform.
- Have received appropriate training with respect to the duties they are to perform.
- Be bound not to disclose sensitive Certificate Authority (CA) security-relevant information or Subscriber information.
- Not be assigned duties that may cause conflict with their Certificate Authority (CA) duties.

5.3.1. Qualifications, Experience, and Clearance Requirements

The PKI requires that personnel performing duties with respect to the operation of a Certificate Authority (CA) have adequate qualifications and experience in Public Key Infrastructures (PKIs). Personnel should meet organizational personnel security requirements. Certificate Authority (CA) administrators should have the following:

- General PKI knowledge and training.
- Information Security knowledge.
- Product specific training.
- No major observations in the background check verification.

5.3.2. Background Check Procedures

Background checks should be performed in accordance with Visa‘s standard organizational Policies and Procedures. People considered for employment are thoroughly screened by an investigative agency:

- Complete criminal background verification
- Complete and verifiable employment history

5.3.3. Training Requirements and Procedures

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

Vettors engaged in Certificate issuance should maintain skill levels consistent with the Visa CA's training and performance programs.

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

The Visa CA should require all Validation Specialists to pass an examination provided by the Visa CA on the information verification requirements outlined in these Requirements.

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

- Information Security and general Public Key Infrastructure (PKI) knowledge
- Certificate Authority (CA) administration and operation
- Certificate Authority (CA) business recovery processes
- Applicable industry and government guidelines.
- Visa Security Compliance training

5.3.4. Retraining Frequency and Requirements

The requirements for training (see "Training Requirements and Procedures") should be kept current to accommodate changes in Certificate Authority (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

In the event that there is job rotation, relevant service account passwords should be changed and individual credentials should be deleted.

5.3.6. Sanctions for Unauthorized Actions

In the event of actual or suspected unauthorized action by someone performing duties with respect to the operation of the PKI, the Certificate Authority (CA) Senior Management should request the suspension of the person's access to the PKI immediately until an investigation is conducted. Further action may be recommended regarding employment status.

The PKI should suspend applicable certificates when a Subscriber fails to comply with obligations set out in the Visa Certificate Policy (CP), this CPS, agreements and/or applicable law.

A Certificate Authority (CA) should suspend a certificate if it suspects that conditions may lead to a compromise of keys or certificates. Revocation of certificates depends on the results of an investigation including pertinent documentation.

5.3.7. Independent Contractor Controls

Contracted personnel fulfilling a Visa PKI role are subject to the same personnel controls as Visa employees, described in the Visa Certificate Policy (CP) and this Certification Practice Statement (CPS).

5.3.8. Documentation Supplied to Personnel

The PKI should make available to its Certificate Authority (CA) support personnel the Visa CP, this CPS, and any specific procedures, documents and contracts relevant to their position. This includes Business Recovery Plans (BRPs) and any other document required by personnel to perform their duties.

5.4. Audit Logging Procedures

Audit log files are generated for events relating to the security of the PKI. Security audit logs are automatically collected. When automatic logging fails, a logbook, paper form and other recordings (camera surveillance) should be used. Unauthorized personnel (vendor, guests) should sign in and out. Security audit logs, both electronic and non-electronic, should be retained and made available for compliance audits as required by law.

5.4.1. Types of Events Recorded

Security type events including physical and logical access, process or configuration changes, generating keys, creating certificates, key usage, and any other event that may be required for auditing purposes should be recorded. The types of events are broken into two categories:

- Physical events such as building and room access
- Logical events such as operating system operations and Certificate Authority (CA) system operations

Physical events may use electronic recording and/or logbooks.

Logical events should be recorded automatically in audit logs at the operating-system level and application level.

Physical Events

For physical events, the following information should be recorded:

- Date and time of event
- Identity of entity/entities
- For guest personnel, the purpose for access (that is, maintenance, upgrades, enhancements, repair, and so on)

The following physical events should also be recorded:

- Access room entry and exit
- Alarm activation
- Equipment sign-out and return
- Certificate Authority (CA) system access

Logical Events

Logical events are divided into Operating System and Certificate Authority (CA) System events. For both events the following should be recorded in the form of an audit record:

- Type of event (application system security, and so on)
- Date and time the event occurred
- Success or failure of event
- Identity of the entity and/or operator of the Certificate Authority (CA) that caused the event
- Any details about the event, such as error information or login message type information

If the PKI application supports signing log files, audit logs may be digitally signed to maintain the information's integrity.

Operating System

Login activity should be logged to the system logs or to a separate access log file. System-level activity (root-level activity or equivalent) should be logged, as appropriate, by the operating system's logging facility.

The following list represents audit events that should be monitored under the operating system for both successes and failures:

- Successful and unsuccessful logon events
- Privileged use and escalation of role/account
- System events
- Critical events
- Emergency events
- System restarts

Certificate Authority (CA) System

The following events monitored should be logged for success and for failure:

- Key generation backup, storage, recovery, archival, and destruction
- Cryptographic device lifecycle management event
- Sign an End-Entity certificate
- Sign a Certificate Authority (CA) certificate
- Issue a Certificate Revocation List (CRL)

- Create a new Certificate Authority (CA)
- Import a Certificate Authority (CA) certificate from Public Key Certificate Standard (PKCS) #12
- Create a new administrator
- Create a new Vettor
- Update a Certificate Authority (CA) certificate
- Reinstate a Certificate Authority (CA) certificate
- Suspend a Certificate Authority (CA) certificate
- Revoke a Certificate Authority (CA) certificate
- Reinstate an End-Entity certificate
- Suspend an End-Entity certificate
- Revoke an End-Entity certificate
- Signing of OCSP responses (delegated to Validation Authority)

Validation requirements

Verification of request set forth in the Visa Global PKI - Vettor Operations Guide.

General Documentation Requirements

The following information pertaining to a Certificate Authority (CA) will be collected either electronically or manually:

- System configuration changes and maintenance
- Personnel changes
- Discrepancy and compromise reports
- Correspondence with Certificate Authority (CA) related external parties such as software and hardware suppliers and network providers as it relates to system maintenance
- Destruction of media containing key material, activation data, or personal Subscriber information

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

Review of audit logs should be conducted periodically. Significant events should be explained. Such reviews involve verifying that the log has not been tampered with, and thoroughly inspecting log entries for any alerts or irregularities. Actions taken following these reviews should be documented.

5.4.3. Retention Period for Audit Log

The PKI audit logs should be retained for a minimum of ninety (90) days and in accordance with Visa Key Controls, specifically Records Management.

5.4.4. Protection of Audit Log

The PKI system configuration and procedures should be implemented together to ensure that:

- Only authorized people have read access to the logs
- Only authorized people may archive or delete audit logs
- Audit logs are not modified

The electronic audit log system should include mechanisms to protect the log files from unauthorized viewing, modification, or deletion. The entity performing audit log archive should not have modification rights and procedures should be implemented to protect archived audit data from deletion or destruction.

Manual audit information should be protected from unauthorized viewing, modification, or deletion. These logs should also be placed in a secure area.

5.4.5. Audit Log Backup Procedures

Audit logs and audit summaries should be backed up, as described, in the Business Recovery Plan (BRP), and placed in a secure area. Any such secondary site should provide adequate protection from environmental threats such as temperature, humidity and magnetic activity.

5.4.6. Audit Collection System (Internal vs. External)

Access to the building, room and/or cage, cabinets, and safes where the Certificate Authority (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. Certificate Authority (CA) system audit processes should be invoked at Certificate Authority (CA) application startup and should end only at Certificate Authority (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 Certificate Authority (CA) operations until the problem is resolved.

The audit collection system is both manual and automatic, as shown in the following table.

Table 5–1: Audit Collection System

Event Collection Point	Automatic/Manual	Recording Entity
Certificate Authority (CA) Facilities	Automatic/Manual	Proximity cards, video, electronic lock with logging, log sheets.
Operating Systems	Automatic	Operating System.
Certificate Authority (CA) Systems	Automatic	Certificate Authority (CA) software Cryptographic Services.
Registration Authority (RA) Systems	Automatic	Certificate Authority (CA) software Cryptographic Services.
Certificate Enrollment Systems	Automatic	Certificate Authority (CA) software Cryptographic Services.

5.4.7. Notification to Event-Causing Subject

When an event is logged, a notice is not required to be given to the individual or entity that caused the event.

5.4.8. Vulnerability Assessments

Events in the audit process are logged to monitor unauthorized activities, system vulnerabilities, and/or compromises. Following an examination of these monitored events, the PKI performs a vulnerability assessment, makes appropriate recommendations to resolve issues, and takes appropriate action.

Visa performs an annual risk assessment that identifies and assesses reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process.

5.5. Records Archival

5.5.1. Types of Records Archived

The PKI archived records should be sufficiently detailed to monitor the proper operation of a Certificate Authority (CA), Registration Authority (RA), and Certificate Enrollment Services and the validity of any certificate (including

those revoked, suspended, or expired) issued by a Certificate Authority (CA).

The following data should be recorded for archive:

- The Visa Public Key Infrastructure (PKI) Key Generation Ceremonies
- Visa Certification Practice Statement (CPS)
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate, revocation and suspension requests
- Subscriber identity authentication data
- Certificates issued
- Certificate Revocation Lists (CRLs) published
- Certificate Related Audit Log information
- Documentation as required by compliance and auditors
- Documents relating to certificate requests and the verification

5.5.2. Retention Period for Archive

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

The minimum retention period for archive data relating to certificate requests, verification and revocation is ninety (90) days after any certificate based on that documentation ceases to be valid.

5.5.3. Protection of Archive

The archive should be protected from unauthorized viewing, modification, or deletion.

The contents of the archive should not be released except as determined by the CRF or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents. Archive media should be stored in a safe, secure storage facility separate from the Certificate Authority (CA) location.

Documents that have reached their end-of-life status should be destroyed following proper disposition rules based on the classification of the document in accordance with Visa Key Controls.

5.5.4. Archive Backup Procedures

Certificates, Certificate Revocation Lists (CRLs), and cryptographic keys should be backed up as part of a Certificate Authority (CA) host system and Business Recovery Procedures (BRP).

5.5.5. Requirements for Time-Stamping of Records

Certificates, CRLs, and OCSP responders should contain time and date information. Time information need not be cryptographic-based.

5.5.6. Archive Collection System (Internal or External)

Archive information is collected internally by Visa.

5.5.7. Procedures to Obtain and Verify Archive Information

The PKI should verify the integrity of the archives at least once every year.

5.6. Key Changeover

If a Certificate Authority (CA) certificate renewal is required (for example, due to expiration), the Certificate Authority (CA) should submit a request for renewal to the appropriate Root Certificate Authority (CA) for signature. The Root Certificate Authority (CA) private key should not be used to sign certificates with a lifetime greater that the lifetime of the Root Certificate Authority (CA) private key.

5.7. Compromise and Disaster Recovery

Information pertaining to business recovery for the PKI should be provided in the Business Recovery Plan (BRP).

5.7.1. Incident and Compromise Handling Procedures

Incident and compromise handling procedures should be provided. For the Information Delivery Certificate Authority (CA), this is the Info Delivery PKI Operations Security Procedures & Practices Guide. For eCommerce and Visa Smart Debit/Credit Certificate Authorities, this is the Visa Certification Authority Incident Management Procedures.

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

In the event of the corruption of computing resources, including software, and/or data, such an occurrence should be reported to the responsible PKI manager and incident-handling procedures should be enacted immediately. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, business recovery procedures may be enacted.

5.7.3. Recovery Procedures After Key Compromise

A confirmed Subscriber key compromise requires immediate revocation.

In the event of the compromise of a Certificate Authority (CA) private key, the following steps should be taken:

- CRF should be notified
- Visa Global Risk Management should be notified
- Subscribers should be notified as soon as practical
- Further action determined by the CRF should be implemented.

5.7.4. Business Continuity Capabilities After a Disaster

The PKI should provide business continuity procedures in a Business Recovery Plan (BRP) that outlines the steps to be taken in the event of a loss of the primary site. The backup site should support minimum capability for PKI Certificate Authorities (CAs).

5.8. CA or RA Termination

In the event that a Certificate Authority (CA) plans to cease operation, it should notify the Visa CRF and the Certificate Authority (CA) Subscribers of its intention at least forty-five (45) days before terminating the service. Certificates should be revoked where there is potential for inappropriate usage; otherwise, certificates may be allowed to expire.

The Certificate Authority (CA) should arrange for the certificate files to be archived for ninety (90) days effective on the publish date of Visa CPS version 3.9 in case of disputes. Private keys used for signing a certificate or Certificate Revocation List (CRL) or for creating a digital signature should not be transferred.

The private keys should be destroyed in accordance with “Private Key Protection and Cryptographic Module Engineering Controls”.

A Certificate Authority (CA) and/or Registration Authority (RA) should arrange for the continued retention of Certificate Authority (CA) keys, final Certificate Revocation List (CRL), and other relevant information as stipulated in “Records Archival” and should notify its Subscribers promptly upon termination of operations.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. CA Key Pair Generation

Certificate Authority (CA) key pair generation should be from a secure cryptographic Host Security Module (HSM) rated at least Federal Information Processing Standard (FIPS) Publication (PUB) 140-2 or 140-3, level 3.

For Visa CA Key Pairs created on the publish date of Visa CPS version 1.0 that are for the operator of the Root Visa CA, the Visa CA SHOULD:

1. Prepare and follow a Key Generation Script.

The Visa CA SHOULD:

1. Generate the keys in a physically secured environment as described in the Visa Certification Practice Statement;
2. Generate the Visa CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. Generate the Visa CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the Visa Certification Practice Statement;
4. Log its Visa CA key generation activities; and
5. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

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

6.1.4. CA Public Key Delivery to Relying Parties

Public keys and certificates are stored in the Certificate Authority (CA) repository. The Certificate Authority (CA) public key is delivered to a Subscriber as part of the issuing process. The format may be Distinguished Encoding

Rules (DER) encoded (binary or base64) or Public Key Cryptography Standard (PKCS) #7 (binary or base64), with or without chain, or EMVCo format depending on the Subscriber's requirements.

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 Parameter Generation and Quality Checking

Certificate Authority (CA) keys should be generated using a random or pseudo-random number generator as described in International Standards Organization (ISO) 9564-1 and International Standards Organization (ISO) 11568-5 that are capable of satisfying the requirements of Federal Information Processing Standard (FIPS) Publication (PUB) 140-2 or 140-3, level 3.

End-Entity key pairs for Visa Business Groups, clients or their agents, destined for use with Visa products and/or services should be generated and protected as detailed 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.

The PKI administrators and Vettors should generate their key pair using their smart card token for PKI functions. The issued certificate for administrative personnel should be stored on their personal token and not in a browser.

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

Certificate Authority (CA) root private keys should be used only for signing certificates and Certificate Revocation Lists (CRLs). The key usage should be set for key certificate signing and Certificate Revocation List (CRL) signing.

See Chapter 7, CERTIFICATE, CRL, AND OCSP PROFILES for key usage.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Subscribers should protect their private keys from unauthorized use by a combination of commercially reasonable cryptographic and physical access control mechanisms.

The private key of an entity should be protected from unauthorized use by a combination of commercially reasonable cryptographic and physical access control mechanisms as defined by this Visa Certification Practice Statement (CPS). The level of protection should be adequate to deter a motivated attacker with substantial resources.

If key recovery is implemented, 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 when stored by the Certificate Authority (CA) protected by cryptographic hardware.

Certificate Authority (CA) Keys should be protected by a secure cryptographic host module rated at Federal Information Processing Standard (FIPS) 140-2 or 140-3, Level 3 or higher.

6.2.1. Cryptographic Module Standards and Controls

Certificate Authorities' (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 Certificate Authority (CA) key generation operations. At a minimum, there should be multi-person control for operational procedures so that no one person can gain control over the

Certificate Authority (CA) signing key. The principle of split knowledge and dual control as outlined in "Trusted Roles" should be applied.

6.2.3. Private Key Escrow

Certificate Authority (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 Certificate Authorities (CAs) should back up Certificate Authority (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 by 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 MAY be generated by and in a cryptographic module. If a cryptographic module is used, CA Private Keys are not exported from the cryptographic module.

6.2.7. Private Key Storage on Cryptographic Module

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

6.2.8. Activating Private Keys

This subsection does not apply to private keys on VSDC ICC cards in the customer's possession. The use of a private key, at a minimum, requires authenticating with a password.

6.2.9. Deactivating Private Keys

This subsection does not apply to private keys on VSDC ICC cards in the customer's possession.

When private 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 automatically deactivates the private key after a pre-set period of inactivity.

6.2.10. Destroying Private Keys

This subsection does not apply to private keys on VSDC ICC cards in the customer's possession.

Upon termination of use of a private key, over-writing should securely destroy copies of the private key in computer memory and shared disk space.

When a root key is removed, the primary HSM on which it resides should be initialized, and tokens used in restoring the key should be destroyed. This also applies to components of keys used to encipher the root key, if applicable. Any such destruction should be witnessed PKI senior manager or designate. A log should be kept of the removal event.

The log should specify the key removed, people attending, time and date, as well as other relevant information, such as Host Security Module (HSM) serial numbers, location, and numbers of tamper-evident bags.

Key material should be maintained under dual control and split knowledge when required.

Keys may include:

- Key Components

- Key Cryptograms
- Key Shares (for example, smart cards with key material)
- Paper-based keying material should be destroyed by crosscut shredding, burning or pulping. Residue should be reduced to 5mm or smaller.

Burned material should be reduced to white ash. Key components stored on other media should be destroyed so that it is impossible to recover by physical or electronic means.

6.2.11. Cryptographic Module Rating

Cryptographic Module‘s used in CA SHOULD be FIPS 140-2 or 140-3 certified.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Issuing Certificate Authorities (CAs) should retain all verification public keys for a period of at least ninety (90) days after any Certificate based on that documentation ceases to be valid.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Transport Layer Security (TLS) end entity certificates issued musshouldt be issued with a maximum validity period as follows:

- For Visa eCommerce: 398 days
- For Information Delivery: 398 days
- For Visa Smart Debit/Credit (VSDC): 10 years
- For Vusa Corporate: 27 months

Key usage periods should be less than or equal to the remaining validity period of a Certificate Authority (CA) certificate’s remaining validity period.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

If activation data is used to protect any Certificate Authority (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.

6.4.2. Activation Data Protection

Authorized users are required to safeguard their activation data in accordance with Visa Key Controls and Data Protection Technical Security Requirements.

6.4.3. Other Aspects of Activation Data

Not applicable.

6.5. Computer Security Controls

6.5.1. Computer Security Requirements

Computer security controls for Certificate Authorities (CAs) should provide protection from unauthorized access, modification, substitution, insertion and/or deletion. These controls should provide protection to help ensure that any such attempts will be prevented or will have a high probability of being detected in a timely manner. The following functionality for Certificate Authorities (CAs) should be provided by the operating system, or through

a combination of operating systems, Certificate Authority (CA) software, and/or physical safeguards (policies and procedures).

Each Certificate Authority (CA) server should include the following functionalities:

1. Access control to Certificate Authority (CA) services.
2. Enforced separation of duties for Certificate Authority (CA) administrative roles.
3. Identification and authentication of Certificate Authority (CA) administrative roles and associated identities.
4. Use of cryptography for session communication and database security.
5. Archival of Certificate Authority (CA) and End-Entity history and audit data.
6. Audit of security related events.
7. Trusted path for identification of Public Key Infrastructure (PKI) roles and associated identities.
8. Recovery mechanisms for keys and Certificate Authority (CA) system.

The CA should enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

S/MIME certificates issued automatically through the user enrollment process should NOT use multi-factor authentication.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

PKIs should use Certificate Authority (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 Certificate Authority (CA) system. Certificate Authority (CA) software, when first loaded should provide a method for a Certificate Authority (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 Certificate Authority (CA) software.

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

6.6.3. Life Cycle Security Controls

6.7. Network Security Controls

The Root Certificate Authorities (CAs) are not connected to any network, and therefore there is no threat of attack through open or general-purpose networks. The exception is VSDC root certificates which are not offline.

The online Issuing Certificate Authorities should use commercially reasonable efforts to protect their servers from attack through any open or general purpose network.

Such 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 Certificate Authority (CA) and the Visa product and/or service.

The PKI servers should be protected by appropriate network security controls. Network security controls should permit only authorized access to the PKI servers. Auditing should be enabled and checked on a periodic basis. Remote access to the PKI environment should be through an authenticated and encrypted connection. No other remote access is permitted to the host platform for system administration unless approved by the Visa Cryptographic Review Forum (CRF). Unnecessary services should be disabled.

The configuration should comply with the relevant Visa Technical Security Requirements (TSRs).

6.8. Time-Stamping

Certificates, CRLs, and OCSP responders contain time and date information.

Time information need not be cryptographic-based.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

7.1.1. Version Number(s)

Certificate Authorities (CAs) 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 Public Key Infrastructure (PKI) End-Entity software supports the base (non-extension) X.509 fields as well as any certificate extensions, as defined in this 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".

Table 7-1 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

7.1.2.1. Root CA Certificate Profile

Certificate Authority Certificates The Public Key Infrastructure (PKI) should support version 3 extensions in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile".

Table 7-2 shows the extensions in the PKI Root CA certificates.

Table 7–2: Public Key Infrastructure and Root CA Certificates

Field	Criticality	Description
Basic Constraint	Yes	Subject Type =cA; Path Length = None
Authority Key Identifier	No	System-generated (Optional)
Subject Key Identifier	No	System-generated
Key Usage	Yes	Digital Signature (keyCertSign, cRLSign)
extendedKeyUsage	No	This extension should NOT be present.

7.1.2.2. Cross-Certified Subordinate CA Certificate Profile

7.1.2.3. Technically Constrained Non-TLS Subordinate CA Certificate Profile

7.1.2.4. Technically Constrained Precertificate Signing CA Certificate Profile

7.1.2.5. Technically Constrained TLS Subordinate CA Certificate Profile

7.1.2.6. TLS Subordinate CA Certificate Profile

7.1.2.7. Subscriber (Server) Certificate Profile

The PKI should support the extensions for Transport Layer Security (TLS) Client certificates, as shown in Table 7-3.

Table 7–3: Extensions for Transport Layer Security Client Certificates

Field	Criticality	Description
Authority Information Access	No	id-adocsp (may), id-adcaIssuers (should)
Authority Key Identifier	No	System-generated
Certificate Policies (CPs)	No	Identifies the Certificate Policy (CP), Object Identifier (OID), Uniform Resource Locator [URL] and/or user notice if different from the Issuing Certificate Authority (CA)
Certificate Revocation List (CRL) Distribution Point	No	Identifies how Certificate Revocation List (CRL) information is published or obtained (Object Identifier (OID), and Uniform Resource Locator [URL] query
Key Usage	Yes	digitalSignature, keyEncipherment, dataEncipherment **
Extended Key Usage	No	id-kp-clientAuth

**For Client certificates not all key usages will be present for all profiles. The usages listed represent possible combinations depending on use case. Visa TLS Root CA and Issuing Certificate Authorities (CAs) does not issue client certificates.

The PKI supports the extensions for Transport Layer Security (TLS) Server certificates, as shown in Table 7-4.

Table 7–4: Extensions for Transport Layer Security Server Certificates

Field	Criticality	Description
Authority Information Access	No	id-adocsp (may), id-adcaIssuers (should)
Authority Key Identifier	No	System-generated
Certificate Policies (CPs)	No	Identifies the Certificate Policy (CP), Object Identifier (OID), Uniform Resource Locator [URL] and/or user notice if different from the issuing Certificate Authority (CA)
Certificate Revocation List (CRL) Distribution Point	No	Identifies how Certificate Revocation List (CRL) information is published or obtained (Object Identifier (OID), and Uniform Resource Locator [URL] query
Key Usage	Yes	digitalSignature, keyAgreement, keyEncipherment**

Field	Criticality	Description
Extended Key Usage	No	id-kp-serverAuth
Subject Alternative Name	No	SubjectAltName should contain at least one: dNSname and/or iPAddress

**For Server certificates not all key usages will be present for all profiles. The usages listed represent possible combinations depending on use case.

The PKI supports the extensions for Transport Layer Security (TLS) Server and Client certificates, as shown in Table 7-5.

Table 7–5: Extensions for Transport Layer Security Server and Client Certificates

Field	Criticality	Description
Authority Information Access	No	id-adocsp (may), id-adcaIssuers (should)
Authority Key Identifier	No	System-generated
Certificate Policies (CPs)	No	Identifies the Certificate Policy (CP), Object Identifier (OID), Uniform Resource Locator [URL] and/or user notice if different from the issuing Certificate Authority (CA)
Certificate Revocation List (CRL) Distribution Point	No	Identifies how Certificate Revocation List (CRL) information is published or obtained Uniform Resource Locator [URL].
Key Usage	Yes	digitalSignature, keyAgreement, keyEncipherment**
Extended Key Usage	No	id-kp-serverAuth and id-kp-clientAuth
Subject Alternative Name	No	SubjectAltName should contain at least one: dNSname and/or iPAddress

**For Server and Client certificates not all key usages will be present for all profiles. The usages listed represent possible combinations depending on use case.

7.1.2.8. OCSP Responder Certificate Profile

7.1.2.9. Precertificate Profile

For purposes of clarification, a Precertificate, as described in RFC 6962 - Certificate Transparency, should not be considered to be a “certificate” subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

7.1.2.10. Common CA Fields

Table 7-8 shows the extensions in the PKI subordinate CA certificates.

Table 7–6: Subordinate CA Certificates

Field	Criticality	Description
Basic Constraint	Yes	Subject Type =cA; Path Length = Use Case Dependent
Certificate Policies	No	Reserved Policy Identier and optional id-qt-cps and other identifiers
CRL Distribution Points	No	Included for issuing and subordinate CAs.
Authority Key Identifier	No	System-generated
Subject Key Identifier	No	System-generated

Field	Criticality	Description
Certificate Policies (CPs)	No	Identifies the Certificate Policy (CP). Object Identifier (OID), Uniform Resource Locator (URL) and/or user notice.
Certificate Revocation List (CRL) Distribution Point	No	Identifies how Certificate Revocation List (CRL) information is published or obtained Uniform Resource Locator [URL].
Key Usage	Yes	keyCertSign, cRLSign
extendedKeyUsage	No	Dependent on use case

7.1.2.11. Common Certificate Fields

7.1.3. Algorithm Object Identifiers

The Certificate Authorities (CAs) should use, and TLS Server Certificates and RPs should support (for signing and verification) the following:

RSA 2048 bit modulus or greater unless approved by the Visa CRF algorithm in accordance with Public Key Cryptography Standard (PKCS) #10. Nist curves P-256 and P-384.

Secure Hash Algorithm (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.

7.1.3.1. SubjectPublicKeyInfo

7.1.3.2. Signature AlgorithmIdentifier

7.1.4. Name Forms

Every DN should be in the form of an X.501 DirectoryString. Certificates issued by a Certificate Authority (CA) should contain the full X.500 Distinguished Name of the certificate issuer and certificate subject in the issuer name and subject name fields.

7.1.4.1. Name Encoding

For every valid Certification Path (as defined by RFC 5280, Section 6) chaining to a Visa Root CA:

- For each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate should be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.
- For each CA Certificate in the Certification Path, the encoded content of the Subject Distinguished Name field of a Certificate should be byte-for-byte identical among all Certificates whose Subject Distinguished Names can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2. Subject Attribute Encoding

CAs that include attributes in the certificate subejct filed that are listed in the table below should encode those attributes follow encoding requirements.

Table 7–7: Base Certificate Revocation List

Attribute	Encoding Requirements
countryName	PrintableString
stateOrProvinceName	UTF8String or PrintableString
localityName	UTF8String or PrintableString

Attribute	Encoding Requirements
organizationName	UTF8String or PrintableString
organizationUnitName	UTF8String or PrintableString
commonName	UTF8String or PrintableString
serialNumber	PrintableString
organizationIdentifier	UTF8String or PrintableString

7.1.4.3. Subscriber Certificate Common Name Attribute

7.1.4.4. Other Subject Attributes

7.1.5. Name Constraints

Subject and Issuer DNs should comply with Public Key Infrastructure Extensions (PKIX) standards and be present in all certificates.

7.1.6. Certificate Policy Object Identifier

Client certificates issued MAY contain the corresponding OID as is defined for the CA or specific profile. See section 1.2.

7.1.6.1. Reserved Certificate Policy Identifiers

7.1.7. Usage of Policy Constraints Extension

The PKI supports the use of the Policy Constraints extension.

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Critical extensions, when applicable, should be interpreted as defined in the Internet Engineering Task Force (IETF) PKIX.

7.2. CRL Profile

7.2.1. Version Numbers

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 following table shows the supported base CRL fields.

Table 7–8: Base Certificate Revocation List

Field	Description
Version	2
Signature Algorithm	The algorithm identifier for the algorithm used to sign the CRL.
Issuer Name	Identifies the entity that signed and issued the CRL.
This Update	This field indicates the issue date of this CRL.
Next Update	The date by which the next CRL will be issued.
Revoked Certificates	Revoked certificates are listed unless there are no certificates revoked in which case the field is absent.

7.2.2. CRL and CRL Entry Extensions

The CA software should correctly process CRL extensions required in the Internet Engineering Task Force (IETF) PKIX Part 1 Certificate and CRL Profile.

The CAs should support and use the CRL Version 2 extensions, as shown in the following table.

Table 7–9: Extensions for Certificate Revocation List Version 2

Field	Criticality	Description
Authority Key Identifier	No	Provides a way to identify the CAs public key that corresponds to the private key used to sign the CRL.
CRL Number	No	The CRL number extension specifies a sequential number for each CRL issued by a CA.
Reason Code	No	Identifies the reason for the certificate revocation.
Invalidity date	No	Date entry extension provides the date on which it is suspected that the private key was compromised

7.3. OCSP Profile

The Online Certificate Status Protocol Profile (OCSP) Responses issued by a CA under this policy should conform to the OCSP profile specified in the IETF RFC 6960 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 RFC 6960.

Certificate status servers (CSSs) operated under this policy should sign responses using algorithms designated for CRL signing, specified in “Certificate Profile”.

7.3.1. Version Number(s)

The CSS operated under this policy should use OCSP version 1, specified in the IETF RFC 6960.

7.3.2. OCSP Extensions

The detailed CRL profiles and the 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

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 CAs 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 such 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 operating under this CPS is adhering to all applicable requirements. The audit will cover requirements that define the operation of a CA under this CPS including:

- CA service integrity, ensuing effective certificate issuance processes and associated policies, key management practices across key lifecycle, and overall certificate lifecycle management as it related to the Visa product or service.
- CA service security, ensuring the appropriate protection of CA operations and the supporting infrastructure.
- CA Governance and compliance, ensuring incident response readiness and procedures, as well as adherence to internal PKI standards and related security requirements.

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 may meet with the CA to determine if the finding can be remedied. An action plan can 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

9.1.1. Certificate Issuance or Renewal 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 RP should be brought to the Pricing Committee's attention.

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) (for example, registration and revocation information, logged events, and correspondence between Subscriber and CA) is considered confidential. 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 should be held only by the Subscriber and should be kept confidential by them. Any disclosure of the private key or media containing the private key by the Subscriber is at the Subscriber's own risk.

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, 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 to be 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 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 of its Subscribers, customers, employees, and partners without the prior consent of the aforementioned unless required by law.

9.4.2. Information Treated as Private

Personal information, not appearing in certificates and in public directories, held by a CA or an RA, (for example, registration and revocation information, logged events, and correspondence between Subscriber and CA) is considered private. 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 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.

9.4.5. 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.

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 Certification Practice Statement (CPS).

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 CPS.

Authentication and validation procedures are implemented, as set forth in Chapter 3, IDENTIFICATION AND AUTHENTICATION of this Visa CPS.

9.6.1. CA Representations and Warranties

The CAs should operate in accordance with the Visa CP, this Visa CPS, and applicable laws as described in "Compliance with Applicable Law", when issuing and managing certificates provided to subordinate CAs, RAs, and Subscribers under the Visa CP.

The CAs should require that the RAs operating on their behalf should comply with the relevant provisions of this Visa CPS concerning the operations of the RAs. The CAs should provide notice of any limitation of liability. See "Indemnities".

The CAs should:

- Issue and administer this Visa CPS that complies with the Visa CP.
- Issue certificates based on requests that are correctly and properly verified according to Chapter 3, IDENTIFICATION AND AUTHENTICATION, if applicable. A CA may delegate this verification, that is, perform due diligence on the certificate requester and certificate request to a RA, but the CA retains responsibility for ensuring that these functions are performed properly.
- Issue certificates only for use in conjunction with those applications that have been 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 CPS 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 CPS. If there are any material changes in the operation of the CA, for example, 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 the Visa CP and this Visa CPS.
- Right to Use Domain Name or IP Address: That, at the time of issuance, an implemented procedure described in the 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) was followed when issuing the Certificate.
- Authorization for Certificate: That, at the time of issuance, the Visa CA implemented a procedure described in the 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 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 CPS, for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading was 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, or, if the Visa CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use.
- Status: a 24x7 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.

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

The CA personnel associated with PKI roles are individually accountable for actions they perform. "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 with respect to the operation and management of any keys, certificates, or hardware and software used in connection with the PKI. Subscribers should also be notified about procedures for dealing with suspected key compromise, certificate or key renewal, and service cancellation.

9.6.2. RA Representations and Warranties

A CA should require that it's RAs, as defined in Chapter 1, INTRODUCTION, comply with the relevant provisions of the Visa CP and this Visa CPS.

The RA is responsible for the identification and authentication of Subscribers according to information in Chapter 3, IDENTIFICATION AND AUTHENTICATION and in Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS. Subscribers' rights and obligations, as well as a description of a Relying Party'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 Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.

The 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 6, TECHNICAL SECURITY CONTROLS.

Vettor personnel are required to undergo an annual compliance validation process as described in Appendix A, SUBSCRIBER AGREEMENTS.

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 is to be performed in a secure manner, as described in Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.

9.6.3. Subscriber Representations and Warranties

The Visa CA should obtain an executed version of the Subscriber Agreement before the issuance of the Certificate. The Subscriber or Terms of Use Agreement should contain provisions imposing on the Applicant itself the obligations and warranties as stated in Appendix A, SUBSCRIBER AGREEMENTS.

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

The Subscriber may only use its key pairs, and the associated certificates issued under a Visa PKI, for the purposes identified in the Visa CP. Key pairs intended for use in a production environment should be generated in that environment in accordance with the Visa CP and this 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.

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

Where a Subscriber knows of, or even suspects, private key compromise, the Subscriber should immediately notify the Issuing CA and/or RA, using the procedures described in Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.

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 makes use of a certificates issued within the Visa PKI. In no event may an RP act in reliance upon a certificate that has expired or been suspended or 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 stated in Chapter 4, CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS. As part of this 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 indemnifications 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 CPS should confer on any third-party any authority to act for, bind, or create, or assume any obligation or responsibility, or make any representation on behalf of another, except as set forth in this Visa CPS. Issuance of certificates in accordance with this Visa CPS does not make a CA or 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, RA, and the Subscriber.

9.8. Limitations of Liability

In no event will a Visa PKI 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 Relying Party Agreements.

Unless otherwise set forth in this Visa CPS and/or Subscriber Agreement and/or Relying Party Agreement, the Subscriber and/or RP hereby 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 and 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 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.

9.9.1. Indemnification by CAs

Notwithstanding any limitations on its liability to Subscribers and RPs, the Visa CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Visa Root CAs do not assume any obligation or potential liability of the Visa CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by RPs or others. Thus the Visa CA should defend, indemnify, and hold harmless each Application Software Supplier for claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the Visa CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the Visa CA where such claim, damage, or loss was directly caused by such Application Software Supplier’s software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the Visa CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2. Indemnification by Subscribers

9.9.3. Indemnification by Relying Parties

9.10. Term and Termination

9.10.1. Term

This Visa CPS remains in force until notice otherwise is communicated by Visa CRF on its website at [https://enroll.visaca.com](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 replacement document, or upon termination of CA operations.

9.10.3. Effect of Termination and Survival

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

9.11. Individual Notices and Communications with Participants

The Visa CRF defines 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 this Visa CPS. Written and signed comments on proposed changes should be directed to the Visa CRF Chairman as described in "Person Determining CPS Suitability for the Policy ". Decisions with respect to the 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 CPS 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 Chapter 1, INTRODUCTION. Decisions with respect to the proposed changes are at the sole discretion of the Visa CRF.

9.12.2. Notification Mechanism and Period

No stipulation.

9.12.3. Circumstances Under Which Object Identifier May Be Changed

Changing 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 should not be held responsible for any delay or failure in performance of its obligations hereunder to the extent such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, acts of terrorism or war, 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

SUBSCRIBER AGREEMENTS

The Visa CA should obtain an executed version of the Subscriber Agreement before the issuance of the Certificate.

The Subscriber or Terms of Use Agreement should contain provisions imposing on the Applicant itself the following obligations and warranties:

- **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 using the procedures described in "Certificate Revocation and Suspension", in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate.
- **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 CA's 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 were to violate 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. The Applicant should also acknowledge that the use of the Visa PKI is subject to the terms and conditions in the Visa Operating Regulations and Procedures or the Operative Commercial Agreement.

Visa has developed the following standard language for its digital certificate Subscriber agreement.

The End-Entity Subscriber agrees that it will:

- 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.
- 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.
- Review and verify the Certificate contents for accuracy.
- Install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to only use the certificate in conjunction with a Visa product or service and to use the Certificate solely

in compliance with applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement.
- Promptly cease using a Certificate and its associated Private Key, and promptly request the Visa CA to revoke the Certificate using the procedures described in "Certificate Revocation and Suspension", in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate.
- 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 or expiry.
- Respond to the Visa CAs instructions concerning Key Compromise or Certificate misuse within one (1) Visa business day for the relevant geographical location.
- Acknowledge and accept that the Visa CA is entitled to revoke the certificate immediately if the Applicant were to violate 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.

For certificates produced from the offline CAs, the Subscriber agreement is a hard-copy and may be a separate document or imbedded in a product participation agreement. For certificates produced from one of Visa's online CAs, the volume makes it impractical to require hard copy agreements. Instead, it is proposed that a "click-through" agreement is used.

For the click-through agreement, the Subscriber agreement would be displayed and the Subscriber would not be able to advance to request the certificate until the Subscriber explicitly accepted the terms. This would be indicated by clicking the box next to the statement "I accept and acknowledge the above terms and conditions." Only after this box had been clicked would the Subscriber be allowed to perform the next step of requesting the certificate.

Digital certificate Subscribers (certificate requesters) can be authenticated in advance of requesting the certificate (pre-authenticated) or after the certificate request has been submitted.

The communication of this information to the Subscriber should be done separately from the certificate request if the Subscriber has been pre-authenticated and a unique identifier and shared secret have been assigned to be used during the online certificate request. The shared secret cannot be included in the same communication that contains the Subscriber agreement.

Before the Subscriber has received the unique identifier (for example, a user ID) and shared secret, the Subscriber can be asked to enter this information before accepting the Subscriber terms. This is accomplished by clicking the box next to "I accept and acknowledge the above terms and conditions." Then the Subscriber unique ID and shared secret can be validated before requesting the certificate.