Visa International
March 2004

Visa Certificate Authority Technical Reference Requirements for VSDC

Version 1.1.1

CONTENTS

FIGURES

Revisions to Version 1.1.1

Section /table	Page	Location	Description
1.4			Updated documentation references to reflect current versions and titles.
1.5			Added reference to valid regional/national service identifiers.
3.			Corrected Appendix from Appendix B to Appendix C
4.1.1			Corrected naming convention for the Issuer Public Key Output File.
4.2.1			Added note that the service identifier of the Visa CA Public Key is always '10 10 00 00' regardless of the service identifier of the Issuer's Public Key Input file.
Appendix A			Updated expiration dates on production Visa CA Public Keys

1. Document Overview

This document describes the interface formats and media requirements for data exchanged between a VSDC Member and the Visa CA (via the Visa regional office of the Member) relating to first-time Issuer registration, certificate request and response, and distribution and migration of the Visa CA Public Keys.

1.1. Audience

The intended audience for this document consists of Members implementing and operating a VSDC program and vendors who develop supporting products or who act as third party providers. The document assumes some knowledge of cryptography.

1.2. Scope

This document describes the formats relating to the international requirements for Members concerning VSDC Issuer Public Key Certificates and Visa CA Public Keys. Individual regions may have specific requirements in addition to those described in this document. Members should contact their Visa Representative for the regional requirements.

VSDC uses Public Key technology and therefore each VSDC Member has to implement and operate systems that support such technology. This involves cryptographic key generation and key management. In this respect a new VSDC Issuer's risk management staff must assess the internal needs of the Issuer and determine the necessary internal processes and procedures as well as requirements to possible third parties.

There are several vendors that supply hardware and software relating to the Public Key technology required for VSDC. Such solutions, or solutions built by the Issuer themselves, must generate files in compliance with Visa's requirements. Visa recommends that new VSDC Issuers who are new to Public Key technology refer to the documentation listed in Section 1.4, and consult with specialists in EMV and Public Key technology as needed.

1.3. Organization of Document

This document contains the following information:

Section 1: Organization of Document

This section.

Section 2: Introduction

Provides an overview of the flow of events when a Member registers for the first time, requests and receives Issuer Public Key certificates, and when a Member requests and receives Visa CA Public Keys.

Section 3: Issuer Certificate Request

Describes the file formats and file names required when a Member requests Issuer Public Key Certificates from their Visa regional office.

Section 4: Response to Issuer Certificate Request

Describes the format of the data the Member can expect back from the Visa CA (via a Visa regional or local office) as a response to a request for Issuer Public Key Certificates. How an Issuer can validate the data received is also described.

Section 5: Retrieving Visa CA Public Keys

Describes how a Member can retrieve and validate Visa CA Public Keys.

1.4. References

Members wishing to participate in VSDC can contact their Visa Representative for the following documents:

Document Reference	Document Full Title, Publication Date, Version
[VIS]	Visa Integrated Circuit Card Specification, Application Overview, Terminal Specification, Card Specification, 31 October 2001
[MIG]	VSDC Member Implementation Guide for Issuers, version 3.0, July 2003
[Visa CA User]	Visa Smart Debit/Credit Certificate Authority User Guide, version 3.3.1, March 2004
[External E-Mail]	Secure Email with External Parties, Inovant, June 1 2001, version 1.0

The following information is available from EMV at the URL http://www.EMVCo.com.

[EMV 2000]	EMV 2000 Integrated Circuit Card Specifications for Payment Systems – Version 4.0, Books 1 – 4
[EMV Iss Sec Guide]	EMV-Issuer Security Guidelines, Version 1.0, 1 July, 2001.

1.5. Terminology and Definitions

Term	Definition
Acquirer	A Visa member that signs a Merchant or disburses currency to a Cardholder in a Cash Disbursement, and directly or indirectly enters the resulting Transaction Receipt into Interchange
Card Authentication	A means of validating whether a card used in a transaction is the genuine card issued by the Issuer
Combined DDA/AC generation (CDA)	A particular way of performing Dynamic Data Authentication, which involves including the Application Cryptogram (AC) in the dynamic signature generated by the ICC. See [VIS] Card Specification, Section 6.4.4.2
Certificate Authority (CA)	In general an entity responsible for establishing and vouching for the authenticity of public keys through issuance and management of public key certificates. For VSDC the VSDC CA that issues Issuer Public Key Certificates
Cryptographic key	The numeric value entered into a cryptographic algorithm that allows the algorithm to encrypt, decrypt, sign or validate the signature of a message
Cryptography	The study of mathematical techniques for providing aspects of information security such as confidentiality, data integrity, authentication and non-repudiation
Data authentication	For VSDC, validation that data stored in the integrated circuit card has not been altered since card issuance. See also Offline Data Authentication.
Decryption	The reversal of the corresponding encryption, a reversible transformation of a cryptogram by a cryptographic algorithm to retrieve the original plain text data.
Data Encryption Standard (DES)	A symmetric algorithm that encrypts blocks of binary data. Defined in FIPS PUB 46-3 'Data Encryption Standard (DES)'
Digest	See 'Hash'
Digital Signature	A transformation of data intended to prove to the data recipient or also to third parties one or both of the following: ▪ Ownership of a particular secret (typically the private component of a public key pair) by the originator of the data ▪ The integrity of the data that was signed
Dynamic Data Authentication (DDA)	This method ensures that Issuer-selected card data elements and transaction-specific dynamic data elements have not been fraudulently altered, and that they come from a valid card
e	In this document used to denote the length, in bytes, of the Issuer Public Key Exponent. There are two valid values for the Issuer Public Key Exponent, viz. 3 and 65537, corresponding to the values 1 and 3 for *e* respectively

Term	Definition
EMVCo	EMVCo, LLC, was formed in February 1999 by Europay International, MasterCard International and Visa International to manage, maintain and enhance the EMV Integrated Circuit Card Specifications for Payment Systems
EMV Integrated Circuit Card Specifications for Payment Systems	Technical specifications developed jointly by Europay International, MasterCard International, and Visa International to create standards and ensure global interoperability for use of chip technology in the payment industry
Hash or hash digest	The result of applying a Hash Algorithm to a piece of input data.
Hash Algorithm	An algorithm used to create a fixed-length output ('digest') from variable length input data. Hash algorithms work for input data of any length. They have the property that it is difficult to find two different input data that have the same digest, and also that given particular output, it is in general difficult to find input that when hashed generates the output. SHA-1 is an example of a Hash Algorithm, and is the one currently used in VSDC
Issuer	A Member that issues cards whose name appears on the card as the Issuer (or, for cards that do not identify the Issuer, the Member that enters into the contractual relationship with the cardholder.)
Offline Data Authentication	A process whereby the card is validated at the point of transaction using RSA Public Key technology to protect against counterfeit or skimming. VIS includes two forms: Static Data Authentication (SDA) and Dynamic Data Authentication (DDA)
Offline Enciphered PIN	A cardholder verification methodology defined in EMV in which the cardholder PIN is entered at a point of sale device, encrypted there with an ICC Public Key, and sent to the ICC where it is validated.
N_{CA}	In this document used to denote the length, in bytes, of the Visa CA Public Key Modulus
N_I	In this document used to denote the length, in bytes, of the Issuer Public Key Modulus
Public Key Infrastructure (PKI)	The total system used in verifying, enrolling and certifying users of a security application
Private Key	The private (secret) component of an asymmetric key pair. The Private Key is always kept in secret by its owner. It may be used to digitally sign messages for authentication purposes
Public Key Exponent	In VSDC either the value 3 or the value 65537.

Term	Definition
Public Key	The public component of an asymmetric key pair. The Public Key is usually publicly exposed and available to users. A certificate to prove its origin often accompanies it. It may be used to verify a message digital signature to authenticate the message sender. In RSA the Public Key consists of the Public Key Exponent and the Public Key Modulus.
Public Key Certificate	An asymmetric transformation of the Public Key by a certification authority and intended to prove to the Public Key recipient the origin and integrity of the Public Key
Public Key pair	The two mathematically related keys, a Public Key and a Private Key which, when used with the appropriate Public Key algorithm, can allow the secure exchange of information and/or message authentication, without the secure exchange of a secret
Registration Authority	In general an entity responsible for verifying the authenticity and authorization of parties requesting public key certificates and for interacting with the CA in servicing those requests
RSA	A Public Key cryptosystem developed by Rivest, Shamir, and Adleman, and widely known as RSA. It is used by VSDC for data encryption and authentication
Service Identifier	Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with hex zeros. Current valid International Service Identifiers are: hex '10 10 00 00' for Credit/Debit hex '20 10 00 00' for Electron hex '30 10 00 00' for Interlink hex '80 10 00 00' for PLUS Valid Regional/National Service Identifiers: Check with your local Visa Regional Office for current list.
SHA-1	A particular hash algorithm. Used in VSDC.
Skimming	The process of copying sufficient data from a credit, debit or ATM card to manufacture a working copy of the card
Static Data Authentication (SDA)	A type of Offline Data Authentication where the acceptance device validates a cryptographic value placed on the card during personalization. This validation protects against some types of counterfeit, but does not protect against skimming
Symmetric Algorithm	An algorithm in which the key used for encryption is identical to the key used for decryption. DES is the best known symmetric encryption algorithm
VSDC Certificate Authority	The Visa certificate authority that certifies VSDC Issuers as participants in VSDC

Term	Definition
Visa Smart Debit/Credit (VSDC)	The Visa service offerings for chip-based debit and credit programs. These services, based on EMV and VIS specifications, are supported by VisaNet processing, as well as by Visa rules and regulations

1.6. Notation

cn	compressed numeric – each byte is used to represent two decimal digits, and the decimal number is padded with trailing hexadecimal FFs'
b	Binary representation
n	numeric– each byte is used to represent two decimal digits, and the decimal number is padded with leading hexadecimal 0's

2. Introduction

This section gives an overview of the flow of events when a Member registers as a VSDC Issuer, requests Issuer Public Key Certificates and receives the response, and when an Acquirer (or Issuer) retrieves Visa CA Public Keys. For a higher-level overview and context, please refer to [Visa CA User Guide], [VIS] and [EMV 2000].

2.1. Flow of Events – Issuer Public Key Certificates

In order for a Member to issue VSDC cards that perform SDA, DDA, CDA, or Offline Enciphered PIN the Member must apply for one or more Issuer Public Key Certificates from the Visa CA.

The Member initiates this process by contacting its Visa regional or country office and requesting the services of the Visa CA. The regional or country office will provide a VSDC Registration Package containing documentation and software that will help the Member prepare their registration and certificate requests.

The Regional Office will also put the Member in contact with a Visa Local Registration Agent, and the Member will then set up a face-to-face registration meeting with this Registration Agent.

The VSDC Registration Package will also detail the process of applying for Issuer Public Key Certificates.

In the subsequent face-to-face meeting with the local or regional office a representative from the Member will submit the registration.

Depending on regional procedures the request for Issuer Public Key Certificates can be submitted at the meeting, or at a later stage.

The Issuer Public Key Certificate Requests will be submitted to a Visa Local Certification Agent appointed to the Issuer by the Regional Office.

The Visa CA will process the requests, and the Region will forward the responses to the Issuer.

This document covers exclusively the file formats and names for the Issuer's requests and the responses coming back to the Issuer, not any intermediate steps which are internal to Visa.

2.2. Flow of Events – Visa Public Keys

The flow of events relating to the dissemination of Visa CA Public Keys is different for Issuers and Acquirers. Issuers will already receive the Visa CA Public Keys in the Registration Package when they register as VSDC Issuers. Acquirers can requests and receive the Visa CA Public Key(s) from their Visa regional office and also download it from Visa's web site.

In the case where the requesting party is an Acquirer, the next step would be to populate all the Acquirer's terminals with the Visa CA Public Key. This is, however outside the scope of this document.

3. Issuer Certificate Request

In order to obtain production or test certificates from the Visa CA a VSDC Issuer submits a VSDC Issuer Public Key Input File to a Local Certification Agent appointed to the Issuer by the Regional Office. The Region will decide which methods of submission are acceptable. This information will be provided to the Issuer in their VSDC Registration Package when they first contact their Regional Office to register as a VSDC Issuer.

Along with each VSDC Issuer Public Key Input File the Issuer must also submit a matching electronic copy of a Work Order (see [Visa CA User Guide], Appendix B.)

3.1. VSDC Issuer Public Key Input File

The VSDC Issuer Public Key Input File is a binary file with format as defined in Table 1 below:

Field Name	Length (bytes)	Description
Unsigned Issuer Public Key Input Extension	$6 + N_I + e$	See Section 3.3. Here N_I is the length, in bytes, of the Issuer Public Key Modulus and *e* is the length, in bytes, of the Issuer Public Key Exponent
Self-Signed Issuer Public Key Data	N_I	See Section 3.4.

Table 1- Contents of VSDC Issuer Public Key Input File

3.2. File Naming Convention

The file name of the VSDC Issuer Public Key Input File must be of the format CC*TTTTTT*.INP, where:

- "CC" is the prefix used for VSDC, and
- *TTTTTT* is the tracking number, which identifies a request for an Issuer Public Key Certificate. The Regional Office will have provided the Issuer with a range of tracking numbers to use. The Issuer must ensure that they use a new tracking number for each request.

Example: CC123456.INP

3.3. Unsigned Issuer Public Key Input Extension

The Unsigned Issuer Public Key Input Extension is the first part of the VSDC Issuer Public Key Input File. The Input Extension provides information about the Issuer Public Key. Table 2 shows the layout of the data.

Field Name	Length (bytes)	Description	Format
Header	1	Hex '22'	b
Length of Issuer Public Key Modulus	1	Length N_I of Issuer Public Key Modulus in hex (number of bytes)	b
Issuer Public Key Modulus	N_I	Issuer's Public Key Modulus	b
Issuer Public Key Exponent Length	1	Length of Issuer Public Key Exponent (Number of bytes). Either hex '01' (for exponent 3) or hex '03' (for exponent 65537)	b
Issuer Public Key Exponent	1 or 3	Issuer Public Key Exponent. Must be either 3 or 65537, that is, hex '03' or hex '01 00 01'.	b
Tracking Number	3	Tracking Number from Visa Financial Institution Registration Form	n 6

Table 2 - Unsigned Issuer Public Key Input Extension

3.4. Self-Signed Issuer Public Key Data

The Self-Signed Issuer Public Key Data, the second part of the VSDC Issuer Public Key Input File, is the Issuer's Public Key Data signed by the Issuer using its corresponding Private Key. The Visa CA uses the Issuer's Public Key to validate the data, some of which is subsequently placed into the Issuer's Public Key Certificate.

Note: Not all data elements provided to the Visa CA are incorporated into the Issuer Public Key Certificate generated by the Visa CA. Those data elements that are not incorporated into the Issuer Public Key Certificate are used for tracking and verification purposes only.

The Self-Signed Issuer Public Key Data is generated as an RSA signature over the data from Table 3 below. Figure 1 illustrates the process.

Field Name	Length (bytes)	Description	Format
Header	1	Hex '23'	b
Service Identifier	4	Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with hex zeros. Current valid International Service Identifiers are: hex '10 10 00 00' for Credit/Debit hex '20 10 00 00' for Electron hex '30 10 00 00' for Interlink hex '80 10 00 00' for PLUS Valid Regional/National Service Identifiers: Check with your local Visa Regional Office for current list.	b
Certificate Format	1	Hex '02'	b
Issuer Identification Number	4	Leftmost three to eight digits from the Primary Account Number (PAN) padded on the right with hex 'F's.	cn 8
Certificate Expiration Date	2	Month and Year (MMYY) after which this certificate is invalid.	n 4
Tracking Number	3	Tracking Number as found on Registration Form	n 6
Hash Algorithm Indicator	1	Identifies the SHA-1 hash algorithm used to produce the Hash Result. This value is hex '01' for SHA-1, as defined in [EMV2000] Book 2 Annex B3.1	b
Issuer's Public Key Algorithm Indicator	1	Identifies the digital signature algorithm to be used with the Issuer's Public Key. The value is hex '01' for RSA as it is used here, as defined in [EMV2000] Book 2 Annex B2.1	b
Issuer Public Key Modulus Length	1	Length N_I of the Issuer Public Key Modulus in hex (number of bytes)	b
Issuer Public Key Exponent Length	1	Length *e* of the Issuer Public Key Exponent in hex (number of bytes). Either hex '01' (for exponent 3) or hex '03' (for exponent 65537)	b
Leftmost part of Issuers Public Key Modulus	$N_I - (39 + e)$	Leftmost $N_I - (39 + e)$ bytes of Issuers Public Key Modulus	b
Issuer Public Key Exponent	*e*	Issuer Public Key Exponent. Is either 3 or 65537, that is, hex '03' or hex '01 00 01'.	b
Hash Result	20	SHA-1 hash of all elements in this table, except Hash Result, that is, of Header through Issuer Public Key Exponent, in the order they appear in the table.	b

Table 3 - Issuer Public Key Data

The Hash Result in Table 3 is a SHA-1 hash of the concatenation of all data elements from Table 3 except Hash Result in the order they appear in the table (see also Figure 1). The hash is only used during the key certification process and is not the same Hash Result that will be incorporated into the Issuer Public Key Certificate.

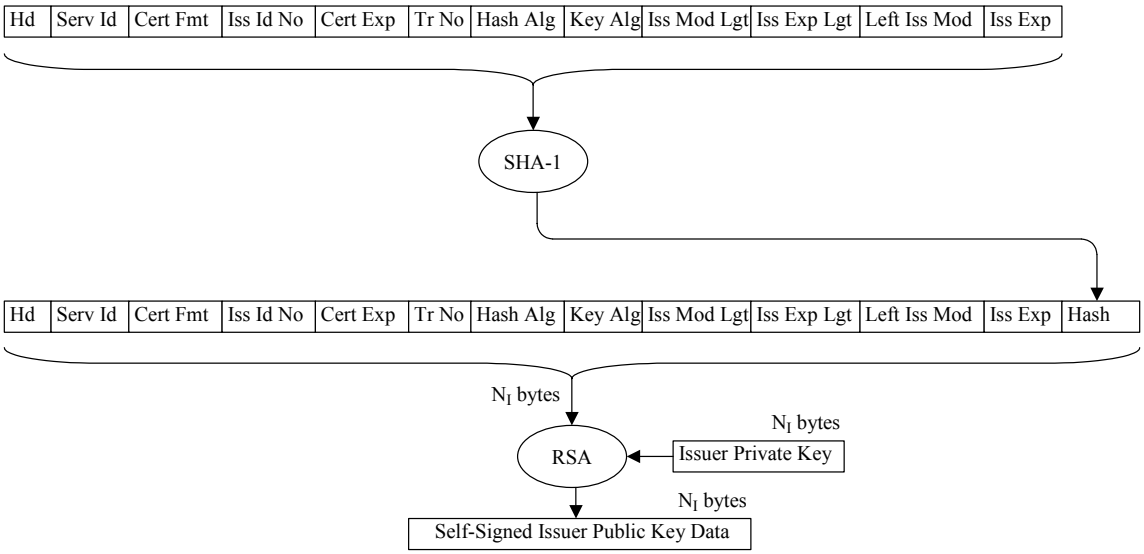

Figure 1 - Generating Self-Signed Issuer Public Key Data

4. Response to Issuer Certificate Request

As a response to an Issuer Certificate Request the Visa CA (via the Visa regional office) provides the Issuer with two sets of files.

The first set consists of one Issuer Public Key Certificate Output File for each valid request for a production or test Issuer Public Key Certificate. Section 4.1 describes the Issuer Public Key Certificate Output File.

The second set consists of one Visa CA Public Key File for each Visa CA Public Key associated with a Visa CA Private Key used to create one of the Issuer Public Key Certificates in the first set. Section 4.2 describes the Visa CA Public Key File.

4.1. Issuer Public Key Certificate Output File

The format of the Issuer Public Key Certificate Output File is defined in Table 4 below.

Field Name	Length (bytes)	Description
Unsigned Issuer Public Key Output Extension	$17+e$ if $N_I \leq N_{CA}+36$ $53+N_I-N_{CA}+e$ if $N_I > N_{CA}+36$, where e, N_I, and N_{CA} are the lengths, in bytes, of the Issuer Public Key Exponent, the Issuer Public Key Modulus, and the Visa Public Key used to create the Issuer Public Key Certificate respectively	See Section 4.1.2
Issuer Public Key Certificate	N_{CA}	See Section 4.1.3
Issuer Public Key Detached Signature	N_{CA}	See Section 4.1.4

Table 4 - Issuer Public Key Output File

4.1.1. File Naming Convention

The Issuer Public Key Certificate Output File is identified by a file name *TTTTTT*.i*NN*, where:

- *TTTTTT* is the tracking number
- i is the letter "I", for "Issuer"
- *NN* is the Visa CA Public Key Index of the Visa CA Public Key used to sign the Issuer Public Key Certificate

Example: 123456.i01.

4.1.2. Unsigned Issuer Public Key Output Extension

The Unsigned Issuer Public Key Output Extension is the first part of the Issuer Public Key Certificate Output File. Table 5 indicates its format. The Output Extension provides information about the Issuer Public Key Certificate.

Field Name	Length (bytes)	Description	Format
Header	1	Hex '24'	b
Service Identifier	4	Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with hex zeros. Current valid International Service Identifiers are: hex '10 10 00 00' for Credit/Debit hex '20 10 00 00' for Electron hex '30 10 00 00' for Interlink hex '80 10 00 00' for PLUS Valid Regional/National Service Identifiers: Check with your local Visa Regional Office for current list.	b
Issuer Identification Number	4	Leftmost three to eight digits from the Primary Account Number (PAN) padded on the right with hex 'F's.	cn 8
Certificate Serial Number	3	Certificate Serial Number assigned by Visa CA	b
Certificate Expiration Date	2	Month and Year (MMYY) after which this certificate is invalid, as defined by the Issuer.	n 4
Issuer Public Key Modulus Remainder Length	1	Length of the Issuer Public Key Modulus Remainder in hex (number of bytes)	b
Issuer Public Key Modulus Remainder	The greater of 0 and ($N_I - N_{CA}$ + 36)	Field only present if $N_I > N_{CA} - 36$, and consists of the $N_I - N_{CA} + 36$ least significant bytes of the Issuer Public Key Modulus. N_I is the length, in bytes, of the Issuer Public Key Modulus and N_{CA} is the length, in bytes, of the Visa CA Key used to create the Issuer Public Key Certificate	b
Issuer Public Key Exponent Length	1	Length *e* of the Issuer Public Key Exponent in hex (Number of bytes). Either hex '01' (for exponent 3) or hex '03' (for exponent 65537)	b
Issuer Public Key Exponent	*e*	Issuer Public Key Exponent. Is either 3 or 65537, that is, hex '03' or hex '01 00 01'.	b
CA Public Key Index	1	Public Key Index for Visa CA Key used to create the Issuer Public Key Certificate	b

Table 5 - Unsigned Issuer Public Key Output Extension

4.1.3. Issuer Public Key Certificate

The Issuer Public Key Certificate is the second part of the Issuer Public Key Certificate Output File. It is generated by signing the Issuer Public Key Certificate Data from Table 6 with the appropriate Visa CA Private Key.

Field Name	Length (bytes)	Description	Format
Recovered Data Header	1	Hex '6A'	b
Certificate Format	1	Hex '02'	b
Issuer Identification Number	4	Leftmost three to eight digits from the Primary Account Number (PAN) padded on the right with hex 'F's.	cn 8
Certificate Expiration Date	2	Month and Year (MMYY) after which this certificate is invalid, as defined by the Issuer	n 4
Certificate Serial Number	3	Binary number unique to this certificate assigned by the Certificate Authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme. For SHA-1 this value is hex '01'	b
Issuer Public Key Algorithm Indicator	1	Identifies the digital signature algorithm to be used with the Issuer Public Key. For RSA as specified in [EMV 2000] Book 2 Appendix A2.1, this value is hex '01'	b
Issuer Public Key Length	1	Length N_I of the Issuer Public Key Modulus, in hex (number of bytes)	b
Issuer Public Key Exponent Length	1	Identifies the length of the Issuer Public Key Exponent in bytes	b
Issuer Public Key Modulus or Leftmost part of the Issuer Public Key Modulus	$N_{CA} - 36$	If $N_I \leq N_{CA} - 36$, this field consists of the full Issuer Public Key Modulus padded to the right with $N_{CA} - 36 - N_I$ bytes of hex 'BB'. If $N_I > N_{CA} - 36$, this field consists of the $N_{CA} - 36$ most significant bytes of the Issuer Public Key Modulus	b
Hash Result	20	SHA-1 hash of the data specified in [EMV 2000] Book 2 Section 5.1 Table 1	b
Recovered Data Trailer	1	Hex 'BC'	b

Table 6 - Issuer Public Key Certificate Data

The Hash Result from Table 6 is calculated over the data specified in [EMV 2000] Book 2 Section 5.1 Table 1.

4.1.4. Issuer Public Key Detached Signature

The Issuer Public Key Detached Signature is the third part of the Issuer Public Key Certificate Output file. It is generated by signing the Detached Signature Data from Table 7 with the same Visa CA Private Key that is used to create the Issuer Public Key Certificate. The signing algorithm is RSA.

Validating the Issuer Public Key Certificate using the Issuer Public Key Detached Signature is optional. The validation should not be a mandatory part of the Issuer's process, as this data structure is being phased out.

Field Name	Length (bytes)	Description	Format
Header	1	Hex '00'	b
Block Format Code	1	Hex '01'	b
Padding Characters	N_{CA} – 38	N_{CA} – 38 bytes of hex 'FF'	b
Separator	1	Hex '00'	b
Algorithm Indicator	15	Hash Algorithm indicator used by the Visa CA	b
Hash Result	20	SHA-1 hash of the concatenation of the Output Extension and the validated Issuer Public Key Certificate	b

Table 7 - Detached Signature Data

The Hash Result from Table 7 is calculated on the concatenation of the Unsigned Issuer Public Key Output Extension (Table 5) and the Issuer Public Key Certificate Data (Table 6).

4.1.5. Validating an Issuer Public Key Certificate

An Issuer may use this method to validate the Issuer Public Key Certificate returned to the Issuer from the Visa CA.

1. If the Issuer Public Key Certificate has a length different from the length of the Visa CA Public Key Modulus, key validation has failed.

2. In order to obtain the Recovered Data (which is the same as the Issuer Public Key Certificate Data) specified in Table 6, use RSA as the recovery function from [EMV 2000] Book 2 Appendix 2.1 to the Issuer Public Key Certificate using the Visa CA Public Key. If the Recovered Data Trailer is not equal to 'BC', key validation has failed.

3. Check the Recovered Data Header. If it is not '6A', key validation has failed.

4. Check the Certificate Format. If it is not '02', key validation has failed.

5. Concatenate from left to right the second to the tenth data elements in Table 6 (that is, Certificate Format through Issuer Public Key or Leftmost Digits of the Issuer Public Key), followed by the Issuer Public Key Remainder (if present) and finally the Issuer Public Key Exponent.

6. Apply the SHA-1 hash algorithm to the result of the concatenation of the previous step to produce the Hash Result.

7. Compare the calculated Hash Result from the previous step with the recovered Hash Result. If they are not the same, key validation has failed.

8. Verify that the Issuer Identification Number is valid. If not, key validation has failed.

9. Verify that the Certificate Expiration Date is correct. If the Certificate Expiration Date is earlier than today's date, the certificate has expired, in which case key validation has failed.

11. If the Issuer Public Key Algorithm Indicator is not '01', key validation has failed.

12. If all the checks above are correct, key validation has passed. Concatenate the Leftmost Digits of the Issuer Public Key and the Issuer Public Key Remainder (if present) to obtain the Issuer Public Key Modulus.

4.2. Visa CA Public Key File

The Visa CA Public Key for VSDC File is a binary file with format as defined in Table 8:

Field Name	Length (bytes)	Description
Unsigned Visa CA Public Key Output Extension	35+ N_{CA}+e_{CA} where N_{CA} and e_{CA} are the lengths, in bytes, of the Visa Public Key Modulus and the Visa Public Key Exponent respectively	See Section 4.2.2
Self-Signed Visa CA Public Key	N_{CA}	See Section 4.2.3

Table 8 - Contents of Visa CA Public Key for VSDC File

4.2.1. File Naming Convention

The Visa CA VSDC Public Key File is identified by a file name *10100000*.V*NN* where:

- *10100000* is the Service Identifier from Table 3
- V is the letter "V", for "Visa"
- *NN* is the Visa CA Public Key Index of the Visa Public Key for VSDC

Example: 10100000.V01

NOTE: The Service Identifier of the Visa CA Public Key is always '10 10 00 00' regardless of the Service Identifier of the Issuer's Public Key as requested in the Issuer's Public Key Input File. The filename of the Visa CA Public Key will always be 10100000.VNN.

4.2.2. Unsigned Visa CA Public Key Output Extension

The Unsigned Visa CA Public Key Output Extension presented in Table 9 is the first part of the Visa CA Public Key File. The output extension provides information about the Visa CA Public Key.

Field Name	Length (bytes)	Description	Format
Header	1	Hex '20'	b
Service Identifier for the Issuer's public key	4	Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with hex zeros. Current valid International Service Identifiers are: hex '10 10 00 00' for Credit/Debit hex '20 10 00 00' for Electron hex '30 10 00 00' for Interlink hex '80 10 00 00' for PLUS For valid Regional/National Service Identifiers, check with your local Visa Regional Office for current list.	b
Length of Visa CA Public Key Modulus	2	Length N_{CA} of Visa CA Public Key Modulus in hex (number of bytes). N_{CA} will be an even number	b
Visa CA Public Key Algorithm Indicator	1	Identifies cryptographic algorithm used to generate the Visa CA Public Key	b
Length of Visa CA Public Key Exponent	1	Length e_{CA} of Visa CA Public Key Exponent in hex (number of bytes)	b

Field Name	Length (bytes)	Description	Format
Registered Application Provider Identifier (RID)	5	Identifies Visa. It is hex 'A0 00 00 00 03'	b
Visa CA Public Key Index	1	Unique Visa CA Public Key Serial Number	b
Visa CA Public Key Modulus	N_{CA}	Visa CA Public Key Modulus	b
Visa CA Public Key Exponent	e_{CA}	Exponent of Visa CA Public Key	b
Hash Results	20	SHA-1 hash of sixth through ninth data elements of this table, that is, RID through Visa CA Public Key Exponent	b

Table 9 - Unsigned Visa CA Public Key Output Extension

4.2.3. Self-Signed Visa CA Public Key

The Self-Signed Visa CA Public Key is the second part of the Visa CA Public Key File. It is created as an RSA signature over the data in Table 10 using the corresponding Visa Private Key.

Field Name	Length (bytes)	Description	Format
Header	1	Hex '21'	b
Service Identifier	4	Identifies a Visa Service. The Proprietary Application Identifier Extension (PIX) is left justified and padded on the right with hex zeros. Current valid Service Identifiers are: hex '10 10 00 00' for Credit/Debit hex '20 10 00 00' for Electron hex '30 10 00 00' for Interlink hex '80 10 00 00' for PLUS For valid Regional/National Service Identifiers, check with your local Visa Regional Office for current list.	b
Registered Application Provider Identifier (RID)	5	Identifies Visa. It is hex 'A0 00 00 00 03'	b
Visa CA Public Key Index	1	Unique Visa CA Public Key Serial Number	b
Certificate Expiration Date	2	Month and Year (MMYY) after which the Visa key represented by this certificate is invalid.	n 4
Visa CA Public Key Algorithm Indicator	1	Hex '01' for RSA as the algorithm used to generate the Visa CA Public Key.	b

Field Name	Length (bytes)	Description	Format
Leftmost portion of the Visa CA Public Key Modulus	$N_{CA} - 36 + e_{CA}$	$N_{CA} - 36 + e_{CA}$ leftmost (most significant) bytes of the Visa CA Public Key Modulus, where N_{CA} and e_{CA} are the lengths of the Visa Public Key Modulus and Visa Public Key Exponent respectively	b
Hash Algorithm Indicator	1	Hex '01' which identifies the SHA-1 hash algorithm used to produce the Hash Result.	b
Visa CA Public Key Exponent Length	1	Length e_{CA} of Visa CA Public Key Exponent in hex (number of bytes)	b
Visa CA Public Key Exponent	e_{CA}	Exponent of Visa CA Public Key	b
Hash Result	20	The SHA-1 hash of the concatenation (from left to right with the high-order byte left) of the following data elements:[1] –Registered Application Provider Identifier (RID) –Visa CA Public Key Index –Visa CA Public Key Modulus –Visa CA Public Key Exponent	b

Table 10 - Visa CA Public Key Certificate Data

4.2.4. Validating Visa CA Public Keys for VSDC

The Hash Result from the Self-Signed Visa CA Public Key can be used to validate the Visa CA Public Key.

Visa CA Public Keys should be validated as follows:

1. Recover using RSA the Visa CA Public Key Certificate Data (see Table 10) using the Unsigned Visa CA Public Key Modulus from the Unsigned Visa CA Public Key Output Extension (see Table 9).
2. Concatenate the following data recovered from the Unsigned Visa CA Public Key Output Extension from left to right (high-order byte on the left):
   - Registered Application Provider Identifier (RID)
   - Visa CA Public Key Index
   - Visa CA Public Key Modulus
   - Visa CA Public Key Exponent
3. Perform a SHA-1 hash on this data.

[1] As noted in [EMV 2000] Book 2 – Security and Key Management, Table 23

4. Compare the results of that SHA-1 hash digest with the hash results obtained from the Self-Signed Visa CA Public Key.
5. Compare the results of that SHA-1 hash digest with the appropriate hash published in this document (Appendix A) and by Visa on
http://international.visa.com/fb/paytech/smartcard/vsmartspecs/ccpspublickey.jsp

5. Retrieving Visa CA Public Keys

The Visa CA Public Keys are available for public download from Visa's website at the URL:

http://international.visa.com/fb/paytech/smartcard/vsmartspecs/ccpspublickey.jsp

The website contains the Visa CA Public Keys as HTML text and also a link to an Adobe format (PDF) document containing the same information.

Before an Acquirer relies on the downloaded information (e.g. by loading it onto their terminal population) the Acquirer must check the information with a secondary source.

Appendix A in this document contains the current Visa CA Public Keys, including a SHA-1 hash digest of each key. As a printed document may be out of date, the keys published in this document must not be relied on as a primary source of the Visa CA Public Keys, but can serve as a secondary source.

Another recommended option for a secondary source is to contact the Visa regional office and request that they send a fax with either the full Visa CA Public Keys, or a SHA-1 hash of each key. In this case the Acquirer must also make reasonable checks that the fax really comes from their Visa regional office.

There are two feasible ways of double-checking the primary source against a secondary source. One is to check the full key (Modulus and Public Exponent) byte-by-byte; another is to recalculate the SHA-1 hash digest over the primary source and compare with the SHA-1 hash digest from the secondary source.

If a key is checked byte-by-byte both the Visa CA Public Key Modulus and the Visa Public Key Exponent must match.

If the SHA-1 hash digests are compared, the Acquirer must themselves calculate a SHA-1 hash digest over each Visa CA Public Key retrieved from the Visa web site, and compare this hash digest with the one from the secondary source (Appendix A in this document or a fax from their Visa regional office).

As specified in [EMV 2000] Book 2 Section 11.2.2, the data that is hashed consists of the concatenation of:

- Registered Application Provider Identifier (RID)
- Visa CA Public Key Index
- Visa CA Public Key Modulus
- Visa CA Public Key Exponent

For each key, it must only be accepted if the two hash digests are identical (all 20 bytes of the hash digest must match.)

These checks are essential and are there to counter the risk of

1. somebody, locally or globally, spoofing the Visa website,
2. the Visa website (or the particular page with the Visa CA Public Keys) being compromised ("hacked") while an Acquirer downloads the keys

Both these threats can result in somebody replacing a Visa CA Public Key with a key of their own choosing.

The Acquirer can also use the checks to verify the continued integrity of the Visa CA Public Keys while they are stored at the Acquirer.

Appendix A—Visa CA Public Keys for VSDC

896 Bit VSDC Production Key

The Visa 896 bit key is scheduled to expire on 31 December 2004.

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	03
Modulus	B3 E5 E6 67 50 6C 47 CA AF B1 2A 26 33 81 93 50 84 66 97 DD 65 A7 96 E5 CE 77 C5 7C 62 6A 66 F7 0B B6 30 91 16 12 AD 28 32 90 9B 80 62 29 1B EC A4 6C D3 3B 66 A6 F9 C9 D4 8C ED 8B 4F C8 56 1C 8A 1D 8F B1 58 62 C9 EB 60 17 8D EA 2B E1 F8 22 36 FF CF F4 F3 84 3C 27 21 79 DC DD 38 4D 54 10 53 DA 6A 6A 0D 3C E4 8F DC 2D C4 E3 E0 EE E1 5F
Exponent	03
Secure Hash Algorithm-1 Hash	FE 70 AB 3B 4D 5A 1B 99 24 22 8A DF 80 27 C7 58 48 3A 8B 7E

1024 Bit VSDC Production Key

The Visa 1024 bit key is scheduled to expire on 31 December 2009.

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	01
Modulus	C6 96 03 42 13 D7 D8 54 69 84 57 9D 1D 0F 0E A5 19 CF F8 DE FF C4 29 35 4C F3 A8 71 A6 F7 18 3F 12 28 DA 5C 74 70 C0 55 38 71 00 CB 93 5A 71 2C 4E 28 64 DF 5D 64 BA 93 FE 7E 63 E7 1F 25 B1 E5 F5 29 85 75 EB E1 C6 3A A6 17 70 69 17 91 1D C2 A7 5A C2 8B 25 1C 7E F4 0F 23 65 91 24 90 B9 39 BC A2 12 4A 30 A2 8F 54 40 2C 34 AE CA 33 1A B6 7E 1E 79 B2 85 DD 57 71 B5 D9 FF 79 EA 63 0B 75
Exponent	03
Secure Hash Algorithm-1 Hash	D3 4A 6A 77 60 11 C7 E7 CE 3A EC 5F 03 AD 2F 8C FC 55 03 CC

1152 Bit VSDC Production Key

The Visa 1152 bit key is scheduled to expire on 31 December 2012.

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	07
Modulus	A8 9F 25 A5 6F A6 DA 25 8C 8C A8 B4 04 27 D9 27 B4 A1 EB 4D 7E A3 26 BB B1 2F 97 DE D7 0A E5 E4 48 0F C9 C5 E8 A9 72 17 71 10 A1 CC 31 8D 06 D2 F8 F5 C4 84 4A C5 FA 79 A4 DC 47 0B B1 1E D6 35 69 9C 17 08 1B 90 F1 B9 84 F1 2E 92 C1 C5 29 27 6D 8A F8 EC 7F 28 49 20 97 D8 CD 5B EC EA 16 FE 40 88 F6 CF AB 4A 1B 42 32 8A 1B 99 6F 92 78 B0 B7 E3 31 1C A5 EF 85 6C 2F 88 84 74 B8 36 12 A8 2E 4E 00 D0 CD 40 69 A6 78 31 40 43 3D 50 72 5F
Exponent	03
Secure Hash Algorithm-1 Hash	B4 BC 56 CC 4E 88 32 49 32 CB C6 43 D6 89 8F 6F E5 93 B1 72

Appendix B—Visa CA Test Public Keys for VSDC

896 Bit VSDC TEST Key

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	98
Modulus	CA 02 6E 52 A6 95 E7 2B D3 0A F9 28 19 6E ED C9 FA F4 A6 19 F2 49 2E 3F B3 11 69 78 9C 27 6F FB B7 D4 31 16 64 7B A9 E0 D1 06 A3 54 2E 39 65 29 2C F7 78 23 DD 34 CA 8E EC 7D E3 67 E0 80 70 89 50 77 C7 EF AD 93 99 24 CB 18 70 67 DB F9 2C B1 E7 85 91 7B D3 8B AC E0 C1 94 CA 12 DF 0C E5 B7 A5 02 75 AC 61 BE 7C 3B 43 68 87 CA 98 C9 FD 39
Exponent	03
Secure Hash Algorithm-1 Hash	E7 AC 9A A8 EE D1 B5 FF 1B D5 32 CF 14 89 A3 E5 55 75 72 C1

1024 Bit VSDC TEST Key

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	99
Modulus	AB 79 FC C9 52 08 96 96 7E 77 6E 64 44 4E 5D CD D6 E1 36 11 87 4F 39 85 72 25 20 42 52 95 EE A4 BD 0C 27 81 DE 7F 31 CD 3D 04 1F 56 5F 74 73 06 EE D6 29 54 B1 7E DA BA 3A 6C 5B 85 A1 DE 1B EB 9A 34 14 1A F3 8F CF 82 79 C9 DE A0 D5 A6 71 0D 08 DB 41 24 F0 41 94 55 87 E2 03 59 BA B4 7B 75 75 AD 94 26 2D 4B 25 F2 64 AF 33 DE DC F2 8E 09 61 5E 93 7D E3 2E DC 03 C5 44 45 FE 7E 38 27 77
Exponent	03
Secure Hash Algorithm-1 Hash	4A BF FD 6B 1C 51 21 2D 05 55 2E 43 1C 5B 17 00 7D 2F 5E 6D

1152 Bit VSDC TEST Key

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	95
Modulus	BE 9E 1F A5 E9 A8 03 85 29 99 C4 AB 43 2D B2 86 00 DC D9 DA B7 6D FA AA 47 35 5A 0F E3 7B 15 08 AC 6B F3 88 60 D3 C6 C2 E5 B1 2A 3C AA F2 A7 00 5A 72 41 EB AA 77 71 11 2C 74 CF 9A 06 34 65 2F BC A0 E5 98 0C 54 A6 47 61 EA 10 1A 11 4E 0F 0B 55 72 AD D5 7D 01 0B 7C 9C 88 7E 10 4C A4 EE 12 72 DA 66 D9 97 B9 A9 0B 5A 6D 62 4A B6 C5 7E 73 C8 F9 19 00 0E B5 F6 84 89 8E F8 C3 DB EF B3 30 C6 26 60 BE D8 8E A7 8E 90 9A FF 05 F6 DA 62 7B
Exponent	03
Secure Hash Algorithm-1 Hash	EE 15 11 CE C7 10 20 A9 B9 04 43 B3 7B 1D 5F 6E 70 30 30 F6