Welcome to

Payment Technology Standards Manual

The *Payment Technology Standards Manual (*formerly, the *Card Technology Standards Manual)* has been reissued.

The Visa *Confidential* label indicates that the information in this document is intended for use by Visa employees, member banks, and external business partners that have signed a Nondisclosure Agreement (NDA) with Visa. This information is not for public release.

Please send questions or comments to buspubs@visa.com.

Effective: 1 September 2002

Payment Technology Standards Manual

Effective: 1 September 2002

Printed on recycled paper.

Contents

About This Manual

Chapter 1 • Personal Identification Number (PIN)

Chapter 2 • Card Verification Value (CVV and iCVV)

Chapter 3 • Card Verification Value 2 (CVV2)

Chapter 4 • ATM and PIN Pad Functions

Chapter 5 • Data Communications Network Security

Chapter 6 • PIN Verification Method

Chapter 7 • DES Key Management

Figures

Tables

About This Manual

Purpose

The *Payment Technology Standards Manual*:

- Describes the standards applied to PINs (personal identification numbers), Cardholder Verification Value techniques, and the management of cryptographic keys. The standards described in this manual apply to Visa interchange transactions only. (Interchange is defined as the exchange of clearing records between members.)
- Describes the guidelines for encoding account and cardholder data on Track 1 and Track 2 of the magnetic stripe of a Visa card. The magnetic stripe requirements conform to International Organisation for Standardisation (ISO) published standards. Regulations covering the physical characteristics of the stripe are referenced.
- Describes Visa Smart Debit/Visa Smart Credit (VSDC) chip and the Track 2 equivalent data, and the Track 1 discretionary data.

NOTE: *Specifications for the physical properties of the magnetic stripe are not covered in this manual. See* Visa International Operating Regulations, Volume III—Card and Marks Specifications *for information.*

Audience

This manual is intended for use by Center Managers, Card Personalization staff, security personnel, and people who need to know the technology and techniques used to create Visa card products or process.

Organization of This Manual

This manual includes the following chapters and appendixes:

Chapter 1, Personal Identification Number (PIN)—Describes PIN issuance standards.

Chapter 2, Card Verification Value (CVV and iCVV)—Describes the computation used to generate the CVV algorithm encoded in Track 1 and Track 2 of the magnetic stripe and on the chip magnetic stripe image. Test data is also included to verify that the CVV algorithm was programmed correctly. iCVV is an optional risk control feature for VSDC chip cards that facilitates detection of skimmed chip data being used to counterfeit magnetic stripe card transactions.

Chapter 3, Card Verification Value 2 (CVV2)—Describes the data components of the computation algorithm. CVV2 is used as an additional means of cardholder verification during voice referrals and for card not present transactions.

Chapter 4, ATM and PIN Pad Functions—Describes the functional requirements that apply to automated teller machines (ATMs) in the Visa ATM Network and point-of-sale (POS) PIN entry devices.

Chapter 5, Data Communications Network Security—Describes the network security techniques implemented in the VisaNet Integrated Payment (V.I.P.) System. The chapter provides an overview of the Data Encryption Standard (DES), the technique of zone encryption, and the formatting of PIN blocks suitable for transmission.

Chapter 6, PIN Verification Method—Describes the PIN Verification Value (PVV) method used by Visa and explains the calculation of a PVV. This chapter does not describe the related Visa PIN Verification Service (PVS).

Chapter 7, DES Key Management—Describes the standards and procedures used to create, store, and convey to Visa the cryptographic keys associated with PINs, PIN Verification values, and Card Verification values.

Appendix A, Track 1 Data—Describes the contents of Track 1 of the magnetic stripe and the chip Track 1 Discretionary Data.

Appendix B, Track 2 Data—Describes the contents of Track 2 of the magnetic stripe and the chip magnetic stripe image.

Appendix C, Exclusive-OR Operation (XOR)—Explains the exclusive-OR logic operation that is used in the key-generation process and in the creation process for some PIN blocks prior to encryption.

Appendix D, Master Forms—Describes and provides copies of the forms used for key management activities.

A glossary and an index are also included in this manual.

Related Publications

The following Visa publication provides an overview of security standards for PIN-based financial transaction interchange. These standards apply to all organizations that acquire or process transactions that contain PINs:

PIN Management Requirements manual which consists of the following two manuals:

- *PIN Security Requirements*
- *PIN Entry Device Security Requirements*

The following Visa publication provides information about V.I.P. System processing, message formats, and field requirements:

V.I.P. System BASE I Processing Specifications

V.I.P. System SMS POS Processing Specifications

V.I.P. System SMS ATM Processing Specifications

October 2000 VisaNet Business Enhancements Member Implementation Guide

The following Visa publication describes security requirements for an entity to operate an Enrollment/Access Control Server in connection with 3-D Secure.

3-D Secure™ Security Requirements—Enrollment and Access Control Servers

The following ANSI and ISO standards are applicable and related to the information in this manual:

Data Encryption Algorithm
ANSI X3.92

Personal Identification Number (PIN) Management and Security
ANSI X9.8

Personal Identification Number Management and Security
ISO 9564

Banking Key Management (Retail)
ISO 11568

Banking—Secure Cryptographic Devices (Retail)
ISO 13491

Modes of Data Encryption Algorithm Operation
ANSI X3.106

Retails Financial Service Symmetric Key Management Part 1: Using Symmetric Keys
ASNI X9.24

Triple Data Encryption Algorithm (TDEA) Modes of Operation
ANSI X9.52

Personal Identification Number (PIN) 1

In a paper-based system, the cardholder's signature is the primary way to identify the person presenting a payment card. Verification is made by comparing the signature on the transaction draft to the signature on the card's signature panel. If the two signatures match, there is a high probability that the cardholder's identity has been verified.

Transactions at certain terminals, such as self-service (cardholder-operated), require different verification procedures. A terminal cannot compare the cardholder's signature against a card's signature panel.

Commonly available technologies support one widespread solution to the problem of cardholder identity verification—a PIN (personal identification number). The verification process begins when the cardholder enters a PIN at an ATM (automated teller machine) keyboard, at a PIN of a point-of-sale (POS) terminal, or at an unattended device that can accept PINs from Visa cardholders.

When the PIN is to be verified online, the PIN entered is encrypted, transmitted, decrypted and compared to a reference PIN available only in the issuer's (or agent's) processing center, or, a cryptographic transformation of the entered PIN is compared against an identical cryptographic transformation of the reference PIN. If the two versions of the PIN match, then there is a high probability that the cardholder's identity has been verified.

When the PIN is to be verified offline, the entered PIN is compared to the PIN stored on the card's chip. If the two PINs match, then there is a high probability that the cardholder's identity has been verified.

The PIN standards in this chapter only apply to VisaNet interchange transactions. Members may develop and comply with their own standards for PINs used in "on-us" transactions.

1.1 Requirement to Issue PINs

All Visa issuers are required to make PINs available to their cardholders. An issuer can assign or issue PINs using the cardholder's selection, derived PINs, randomly-generated PINs, or any other method deemed suitable by the issuer. Regardless of the method used, it is important that the PIN values be secured and maintained in a way that only the cardholder knows the PIN or has the capability to access the PIN outside a physically secure device.

1.2 PIN Length

The minimum PIN length is four digits. For verification purposes in interchange transactions, the maximum PIN length is six digits.

An issuer can elect to support longer PINs—up to a maximum of 12 digits as specified in *Personal Identification Number Management and Security*, ISO 9564. However, ATM acquirers are *not* obligated to support PINs of more than six digits.

Refer to Chapter 4, ATM and PIN Pad Functions, for the length requirements applicable to acquirer ATMs and PIN entry devices at the point of sale.

NOTE: *Acquirers for Visa EMV-compliant products where PINs are accepted must support PIN lengths in accordance with EMV specifications.*

1.3 PIN Character Set

The PIN entered by the cardholder can consist of numeric digits 0 through 9, alphabetic characters A through Z, or a combination of both. PINs are always numeric. The cardholder may use alpha to remember the PINs but PINs do not contain alpha characters. See ISO 9564.

When entering an alphabetic PIN character, the cardholder selects the key labeled with the corresponding alphabetic character. If the keys are not labeled with alphabetic characters, the cardholder selects the appropriate numeric key after converting the alphabetic character to a numeric digit as shown in Table 1–1. The mapping conforms to standards specified in ANSI X9.8.

NOTE: *Because alphabetic characters differ in various markets and the location of alphabetic characters varies according to different standards, issuers are encouraged to assign numeric PIN values. See above; PIN character set is 0–9.*

ATM keyboard and point-of-sale PIN entry device layouts supporting this alphanumeric correspondence are referenced in Chapter 4.

Table 1–1: Mapping of Alphabetic Characters to Numeric Digits

Alphabetic	Numeric
ABC	2
DEF	3
GHI	4
JKL	5
MNO	6
P	7
Q	1
RS	7
TUV	8
WXY	9
Z	1
—	0

1.4 PIN Security

The value of a PIN as a means of cardholder identification depends on the ability to ensure that the PIN is known only to the cardholder. Issuers must have assurance that PINs will not be compromised when they are used in other members' equipment or facilities.

The following standards provide for PIN security in interchange transactions. These standards apply only when an interchange PIN is outside the issuer's equipment and facilities. The techniques, procedures, and standards used by issuers in their own environment are at the issuers' discretion.

- A PIN used in interchange transactions must never be in a comprehensible (unencrypted form except within a physically secure device or a minimally acceptable PIN Entry Device as described in ISO 9564.
- A PIN used in interchange transactions must be managed using the requirements set forth in the *PIN Management Requirements* manual.

Card Verification Value (CVV and iCVV) 2

This chapter describes the algorithm used to calculate the Card Verification Value (CVV) that is encoded in the Visa-reserved field in Track 1 and the Discretionary Data field in Track 2 of the magnetic stripe or the chip magnetic stripe image. This chapter also describes the calculation for iCVV.

The CVV provides a cryptographic check on the contents of the magnetic stripe. The CVV is generated using secret keys and the algorithm described in this chapter. The algorithm is implemented in a security module or other facility especially designed for highly secret cryptographic operations.

In addition to the algorithm, this chapter includes test data that can be used to verify that the algorithm was implemented correctly. The prerequisites and algorithm for generating the CVV are the same for Track 1 and Track 2 of the magnetic stripe.

CVV is required to be encoded on Track 1 and Track 2 of the magnetic stripe and on the chip magnetic stripe image.

iCVV is an optional Visa Smart Debit/Visa Smart Credit (VSDC) risk control feature that facilitates detection of skimmed chip data being used to counterfeit magnetic stripe cards. Issuers may elect to implement an iCVV encoded in the track data stored on the chip that is different from the CVV encoded on the magnetic stripe.

The iCVV computation is identical to that for the CVV except that the value 999 is used for the service code when calculating the iCVV.

2.1 CVV

2.1.1 DES Algorithm

The CVV computation uses the Data Encryption Standard (DES) algorithm defined by the National Institute of Standards and Technology (NIST). The standard requires a pair of 64-bit cryptographic key; that is, two 64-bit DES keys, each having odd parity and constructed as described in Chapter 5, Data Communications Network Security.

A description of the DES algorithm is beyond the scope of this document. Readers who need technical details should obtain a copy of the standard. See “Related Publications” in the About This Manual.

2.1.2 Generating and Verifying the CVV

The CVV computation generates a three-position CVV for the Visa-Reserved field of Track 1 and the Discretionary Data field of Track 2.

One pair of 64-bit cryptographic keys called Card Verification Keys (CVKs) is used to generate and verify the CVVs for tracks 1 and 2. The issuer sends these keys to Visa under the issuer’s existing Zone Control Master Key (ZCMK). Chapter 7 describes how to generate and manage DES keys.

Visa mandates the following security precautions for CVV keys:

- Issuers must not use the same verification keys for CVV and CVV2 as those used for PIN Verification values (PVVs) with Visa’s PIN Verification Service. If the common keys were to be compromised, it would affect both the issuer’s PVVs and CVVs.
- CVV and CVV2 verification keys should be different from any other DES keys used by the issuer. Because each issuer has unique keys, a breach of security will be limited to a particular issuer rather than affecting all issuers using the CVV.

NOTE: *Using the same key for CVV, iCVV and CVV2 is an exception to the general rule against using one key for multiple applications. The exception is allowed in order to facilitate possible future enhancements to the VisaNet service offerings.*

To create a CVV, the CVK pair is introduced to the DES algorithm with other data. Similar to any DES-based scheme, the security of the output value depends on the secrecy of the DES keys.

The CVK pair must be kept secret and should not be known to anyone. If the unauthorized disclosure of a CVK pair is known or suspected, the CVK pair should be replaced immediately. Cards with CVVs generated using the potentially compromised keys should be reissued as soon as possible. When all such cards have been reissued, the potentially compromised CVK pair should be invalidated. To facilitate changing a member's CVK pair for any reason, Visa can support multiple CVK pairs for each issuer. The VisaNet Integrated Payment (V.I.P.) System can support two CVK pairs online.

2.1.3 Computing the CVV

Throughout the CVV computation, the first of the two 64-bit DES keys is referred to as Key A, the second as Key B. The following steps are performed to compute the CVV:

1. Construct a string of bits by concatenating, from left to right, the right-most four bits of each character of the following data elements:

   – Primary Account Number (PAN)

   – Card Expiration Date

   – Service Code

For example, a 16-digit PAN with a 4-digit Card Expiration Date and a 3-digit Service Code would produce a 23-character (16 + 4 + 3) string that is 92 bits long (23 × 4).

NOTE: *Track 1 and Track 2 data is encoded using the 4-bit patterns shown as b4 to b1 in Table A–1 and Table B–1. For example, the pattern for 4 is 0100, thus the bits selected in step 1 will also be 0100.*

2. Type the result from step 1 into a 128-bit field, right-filling the remaining bits with binary zeros.

   For example, a 16-digit PAN with a 4-digit Card Expiration Date and 3-digit Service Code requires 36 trailing zeroes to complete the 128-bit field.

NOTE: *Valid Service Code and Expiration Date values are described in Appendix A and Appendix B.*

3. Split the 128-bit field into two 64-bit blocks. The left-most 64 bits are Block 1, the right-most 64 bits are Block 2.

4. Encrypt Block 1 using Key A.

5. Exclusive-OR (XOR) the result of step 4 with Block 2. Encrypt this value with Key A. The XOR operation is described in Appendix C.

6. Decrypt the result of step 5 using Key B.

7. Encrypt the result of step 6 using Key A.

8. Use the result of step 7 and, beginning with the left-most digit, extract all the digits from 0 through 9. Left-justify these digits in a 64-bit field.

9. Use the result of step 8 and, beginning with the leftmost digit, extract the hexadecimal digits from A to F. Then, convert each extracted digit to a decimal digit by subtracting 10.

   When converted, hexadecimal B becomes decimal 1. (Hexadecimal B = 11 decimal; 11 - 10 = 1)

10. Concatenate the decimalized digits from step 9 to the right of the result of step 8.

11. Select the three left-most digits. These digits are the CVV which is encoded on the magnetic stripe.

For the first set of test data for a 16-digit account number, the calculation of the CVV is performed as listed in Table 2–1. The values used in the calculation are as follows:

PAN: 4123 4567 8901 2345

Expiration Date: 8701

Service Code: 101

Table 2–1: CVV Calculation Example

CVV Calculation Steps	Example
1. Extract data	Extracted = 4123456789012345 8701 101
2. Place into 128-bit field padded to the right with binary zeros	Padded = 4123456789012345 8701 101 00000 0000...0
3. Split field into two 64-bit blocks	Block 1 = 4123 4567 8901 2345 Block 2 = 8701 1010 0000 0000
4. Encrypt Block 1 using Key A	Block 1 = 4123 4567 8901 2345 Key A = 0123 4567 89AB CDEF Step 4 Result = B76A DDCE 71CC C6BE
5. XOR the result of step 4 with Block 2, then encrypt the XOR result with Key A	Block 2 = 8701 1010 0000 0000 XOR Result = 306B CCDE 71CC C6BE Key A = 0123 4567 89AB CDEF Step 5 Result = BAE6 746F 6DE1 F0E6
6. Decrypt the result of step 5 with Key B	Key B = FEDC BA98 7654 3210 Step 6 Result = B262 ABCB 9DE9 9A63
7. Encrypt the result of step 6 with Key A	Key A = 0123 4567 89AB CDEF Step 7 Result = 8D56 25FA 7801 1A0C
8. Extract all digits from 0 through 9 from the result of step 7	Step 8 Result = 8562 5780 110
9. Extract the hexadecimal digits from the result of step 8 and convert them to numerics by subtracting 10 from each	Extract Hex Digits = DFAA C Step 9 Result = 3500 2
10. Concatenate the result of step 9 to the result of step 8	Concatenate = 8562 5780 1103 5002
11. Select the three left-most digits as the CVV	CVV = 856

2.1.4 Encoding the CVV in Tracks 1 and 2

The CVV must be encoded in positions 3 to 5 of the Visa-reserved field in Track 1 of the magnetic stripe and in any three contiguous positions of the Discretionary Data field in Track 2 of the magnetic stripe. Visa recommends that the CVV be encoded as the first three positions of the Discretionary Data field.

2.1.5 Test Data

The following test data can be used to verify that the CVV algorithm was programmed correctly. The same keys are used with all the test data:

Key A: 0123 4567 89AB CDEF

Key B: FEDC BA98 76543210

Table 2–2: CVV Test Data—16-Digit PAN

16-Digit Primary Account Number	Expiration Data	Service Code	CVV[1]
4123 4567 8901 2345	8701	101	856
4999 9888 8777 7000	9105	111	245
4666 6555 5444 4111	9206	120	664
4333 3222 2111 1222	9307	141	382

[1] Generated values.

2.2 iCVV – Alternate Card Verification Value for Visa Smart Debit/ Visa Smart Credit (VSDC) Chip Transactions

The Card Verification Value (CVV) program has long fulfilled a need to reduce the risk of fraudulent Visa cards by providing a cryptographic check on the validity of the magnetic stripe in an online authorization. There is some concern that chip-based processing might lessen the value of the CVV concept if the magnetic stripe image on the chip card (or transaction) were copied to a traditional magnetic stripe card, thus creating a fraudulent magnetic stripe card with a valid CVV value. To protect against this possibility, the optional Alternate Card Verification Value or iCVV concept has been implemented. However, issuers may continue to encode the CVV on the chip to be identical to that on the magnetic stripe.

Using this concept: if the iCVV value is received on a magnetic stripe-initiated transaction, the CVV validation will fail. The new iCVV concept requires:

- No new information on the magnetic stripe.
- No new information on the chip image of the magnetic stripe.
- No new cryptographic keys and associated key management.
- No changes to merchant and acquirer processing.
- No changes to Host Security Modules.

The new iCVV uses the:

- Same CVV algorithm.
- Same network and Host Security Module messages.
- Same CVV DES key(s) and management.

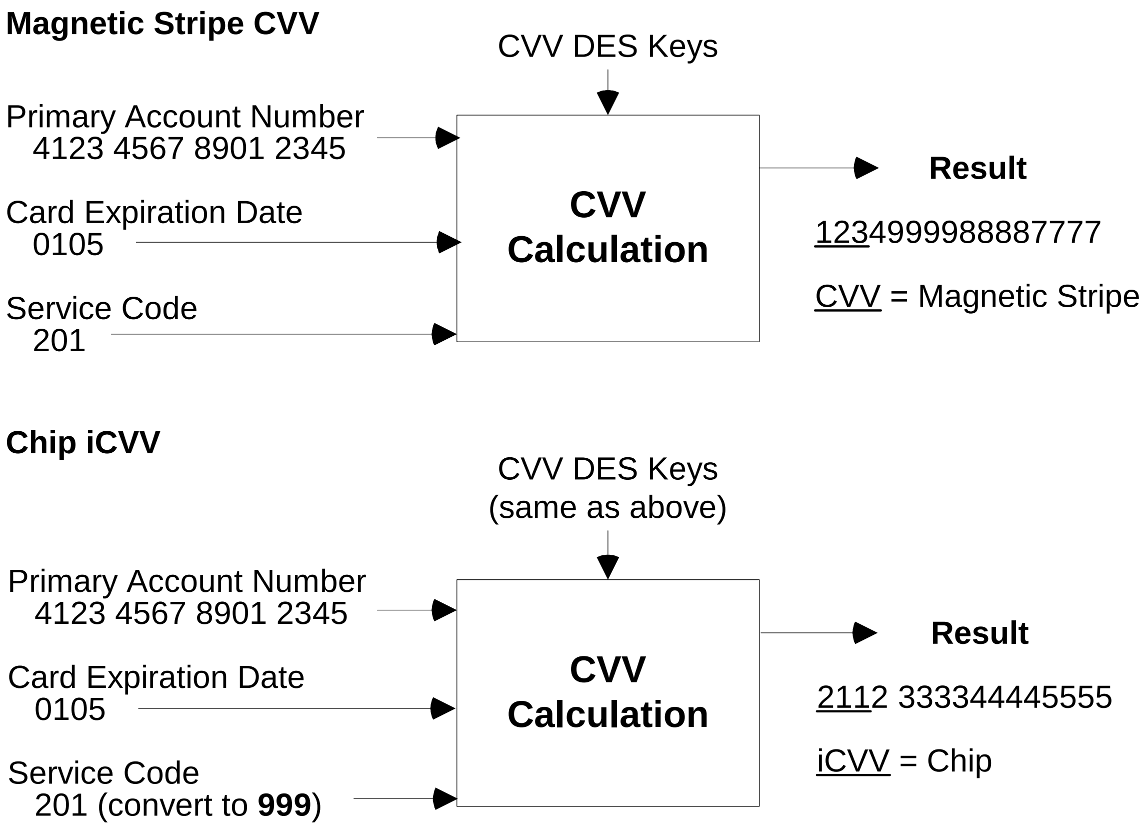
Simply stated, the issuer manipulates one of the pieces of data used to create the CVV value prior to calculation or validation.

The Service Code used in calculating the CVV value for the magnetic stripe CVV is replaced, (only for the calculation of the iCVV), with a value of 999 to create the new iCVV for the magnetic stripe image in the chip. This manipulation is required in the iCVV creation *and* validation.

The CVV remains unchanged on the physical magnetic stripe and the new iCVV value takes its place on the magnetic stripe image information contained in the chip.

The following figure demonstrate the simple difference between the calculation of a magnetic stripe CVV and chip iCVV.

Figure 2–1: Calculation of a Magnetic Stripe CVV and Chip iCVV



NOTE: *The information is only an example; it does not reflect valid CVV or iCVV values.*

Card Verification Value 2 (CVV2) 3

The Card Verification Value 2 (CVV2) is a card verification tool designed to reduce fraud losses on transactions when the card is not present, such as in Mail Order/Telephone Order (MOTO) and electronic commerce (EC) transactions, and to enhance the effectiveness of voice referrals.

Cardholders performing a MOTO/EC transaction may be requested to enter the CVV2 printed on the back of the card. When a voice referral response is received in response to an authorization request, the clerk at the point of sale (POS) may be instructed to read the CVV2 value printed on the back of the card to the referral operator. The Primary Account Number (PAN) and expiration date are then used to calculate a transaction CVV2 value, which is compared to the reference value printed on the card. A match enhances the probability that the genuine card is present at the point of transaction.

The CVV2 value is computed using the same algorithm for the Card Verification Value (CVV) described in Chapter 2, with the exception of the expiration date which is input using embossed or printed format (MMYY).

The Card Verification Key pair used for calculating the CVV2 *may* be the same as the one used to calculate the CVV.

NOTE: *Using the same key for CVV, iCVV and CVV2 is an exception to the general rule against using one key for multiple applications. The exception is allowed in order to facilitate possible future enhancements to the VisaNet service offerings.*

3.1 Data Components

The following data components are used to compute the algorithm:

- Primary Account Number (PAN)
- Card expiration date as it appears on the front of the card (MMYY)
- Three zeros, which take the place of the Service Code value

These three components are encrypted using the Data Encryption Standard (DES) algorithm and a Card Verification Key (CVK) pair, which result in a three-digit, CVV2 value.

Refer to the product-specific VisaNet Integrated Payment (V.I.P.) System processing specifications manuals for specific details.

ATM and PIN Pad Functions 4

This chapter describes the standards applied to ATM (automated teller machine) keyboard and PIN (personal identification number) pad functions.

The requirements in this chapter apply to online VisaNet interchange transactions originating from ATMs or point-of-sale (POS) terminals with encrypting PIN pads. Members may process on-us transactions according to their own requirements.

4.1 ATM Standards and Requirements

There are standards and requirements for ATMs in the Visa ATM Network and PIN POS entry devices in the following areas:

- PIN Length
- PIN Block Format
- PIN Block Encryption
- Security Requirements
- Keyboard Layout

Each of these topics is described separately in the following sections.

4.1.1 PIN Length

ATMs and POS PIN entry devices must be able to accept PINs between four and six digits in length. If an entered PIN exceeds six digits, the acquirer is permitted to truncate the entry to a maximum of six digits.

An issuer can elect to support longer PINs—up to a maximum of 12 digits, as specified in *Personal Identification Number Management and Security*, ISO 9564. However, acquirers are not obligated to support PINs of more than six digits.

NOTE: *Acquirers for Visa EMV-compliant products where PIN is accepted must support PIN lengths in accordance with EMV specifications.*

4.1.2 PIN Block Format

PIN pads accepting PINs for VisaNet Integrated Payment (V.I.P.) System transactions must use ISO PIN Block Format 0 (equivalent to ANSI PIN Block Format 0) to create a PIN block prior to encryption. This format mathematically combines the PIN with part of the PAN. PIN block details are described in Chapter 5, Data Communications Network Security.

When the POS terminal that supports PIN entry is not directly connected to VisaNet, the PIN pad may use ISO PIN Block Format 0 or ISO PIN Block Format 3. However, for the acquirer that is directly connected to VisaNet, the acquirer must encrypt and reformat interchange PINs again using ISO PIN Block Format 0 before transmitting to VisaNet.

NOTE: *ISO PIN Block Format 0 and Visa PIN Block Format 01 are identical. Offline PIN requires the use of ISO PIN Block Format 2.*

4.1.3 PIN Block Encryption

All PINs in exchange messages must be encrypted before transmission. The ANSI X.9.24 standard recognizes the following methods of key management for use in the encryption of PINs at PIN Entry Devices (PEDs):

- Key Management Methods Requiring Compromise Prevention Controls
  - Fixed Transaction Keys
  - Master Keys/Transaction (Session) Keys
- Key Management Method Requiring Compromise Detection Controls
  - Derived Unique Key Per Transaction (DUKPT)

4.1.4 Security Requirements

Security requirements for PIN processing are described in the *Visa PIN Management Requirements* manual

The ATM must be a physically secure device as described in ISO 9564.

The ATM or ATM controller must use a Visa-approved reversible encryption algorithm to encrypt PINs in interchange transactions. Currently, the only approved algorithms are the Data Encryption Standard (DES) and the Triple DES (TDES).

Refer to Chapter 5, Data Communications Network Security, for more information on network security. Chapter 5 also describes the PIN block formats recognized by Visa.

4.1.5 Keyboard Layout

In the U.S., an ATM keyboard must conform to the standard alphanumeric layout shown in Figure 4–1. Outside the U.S., the numeric keys must be placed as shown in Figure 4–1. The alphabetic characters are recommended, but not required.

The POS PIN pad's numeric layout must conform to the layout illustrated in Figure 4–2. The words Clear and Enter can be stated in the local language. The alphabetic characters are recommended but not required. Visa recommends using yellow for the **CLEAR** key and green for the **ENTER** key. A privacy shield is also recommended.

Figure 4–1: Standard ATM Keyboard Layout

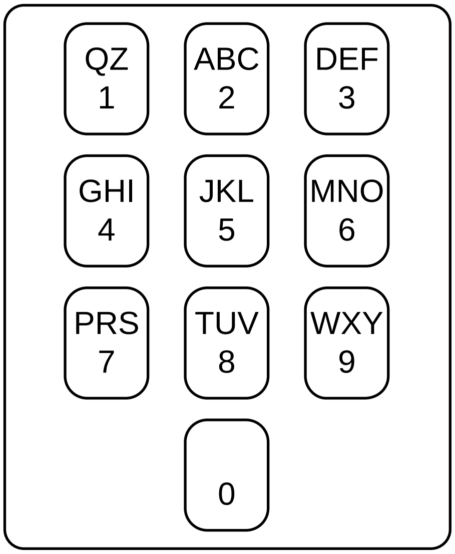
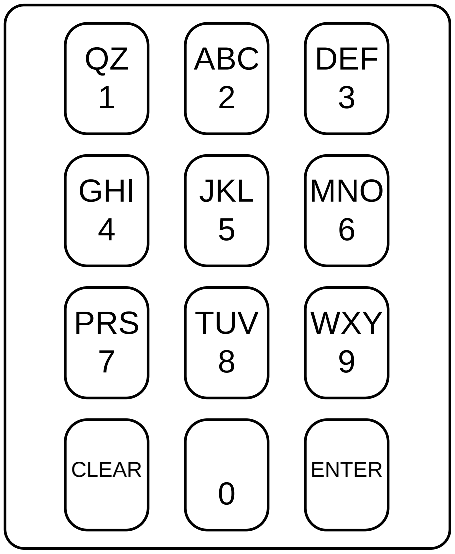


Figure 4–2: POS PIN Pad Layout



Data Communications Network Security 5

The value of a PIN (personal identification number) for cardholder identification depends on its secrecy. Therefore, an unencrypted PIN must not exist outside of a physically secure device or of the issuer's facility.

NOTE: *Visa requires that the PIN value be secured and maintained in a way that only the cardholder knows the PIN or has the capability to access the PIN outside of a physically secure device.*

Because PINs are susceptible to disclosure during inquiry message transmissions, a data communications network must use encryption to protect PINs when they are not within a physically secure device. The network standards for PIN transmission cover the following areas:

- The cryptographic algorithm used to protect data
- The data element to be protected
- The security technique or manner in which the algorithm and data are used

5.1 Cryptographic Algorithm

A cryptographic algorithm used to disguise PINs during Visa interchange transactions must be both secure and reversible. An algorithm is reversible if it is possible to recreate (decrypt) the original data (cleartext) from the encrypted data (ciphertext) by executing the algorithm in reverse.

Visa International is solely responsible for determining if an algorithm provides enough security for use with VisaNet interchange transactions.

Currently, the Data Encryption Standard (DES) and Triple DES (TDES) algorithms are the only algorithms that meet Visa's requirements for security and reversibility for PINs associated with magnetic stripe cards.

The DES specifies using a complex set of mathematical functions to encrypt data. For the encryption process, input to the DES algorithm consists of the following:

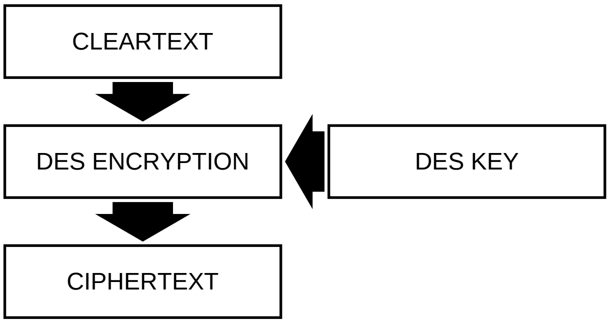
- The data to be encrypted (cleartext)
- A secret cryptographic key

The cleartext must be input as a 64-bit block of data. For online PIN transactions, a PIN must be padded to 64 bits as described in "ISO PIN Block Format 0 or ISO PIN Block Format 3." The cryptographic key is also input as a 64-bit block of data. The key itself is 56 bits long; the other 8 bits are used for parity.

The algorithm outputs a 64-bit block of encrypted data (ciphertext). The cryptographic key governs the process through which cleartext is transformed into ciphertext. Knowing the cleartext and corresponding ciphertext will still not allow the key to be determined in an economically feasible process. An overview of DES encryption is provided in Figure 5–1.

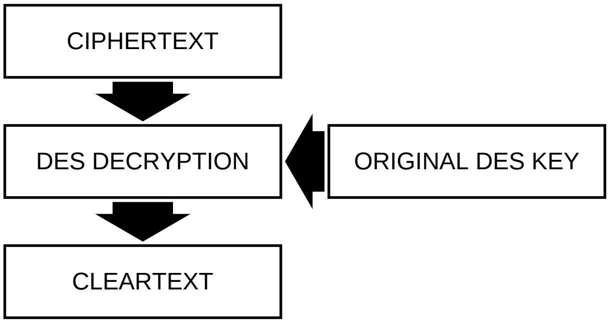
NOTE: *For a description of Triple DES, please refer to ANSI X9.52.*

Figure 5–1: DES Encryption Overview



Ciphertext can be deciphered only by reversing the DES algorithm and by applying the original key used in the encryption process. If the incorrect key is used to decrypt data, the DES algorithm will yield a cleartext result that differs from the correct value. An overview of DES decryption is provided in Figure 5–2.

Figure 5–2: DES Decryption Overview



The secrecy of the enciphered data is based entirely on the secrecy of the DES key. The algorithm itself is not a secret procedure.

Using DES requires the provision of adequate physical security. Therefore, DES keys must be created, stored, and applied in a secure manner. Refer to Chapter 7, DES Key Management, for the Visa standards.

DES also specifies the implementation method required for adequate security. Physical security is needed to protect both cleartext and DES keys during the mathematical transformation. In most cases, a software implementation of DES in standard computer systems does not provide adequate protection from electronic fraud.

5.2 Data Element Protection

The PIN is the only data element in an interchange transaction that must be kept secret. Therefore, all PINs in interchange messages must be encrypted before transmission.

5.2.1 ISO PIN Block Format 0

NOTE: *ISO PIN Block Format 0 and Visa PIN Block Format 01 are identical.*

Before a PIN can be encrypted or decrypted using the DES algorithm, it must be mapped into a block of 64 bits. Only hexadecimal characters are permitted in this PIN block.

The mapping of a PIN to a PIN block must be done using either ISO Format 0 or ISO Format 3 because they are far more secure than any other formats. PIN Block Format 0 is based on the PIN, the PIN length, a subset of the Primary Account Number (PAN), and the pad characters 0 and F, combined through an exclusive-OR (XOR) operation.

The PIN length, which must be expressed as a hexadecimal value, is needed to build a PIN block. For example, if a PIN is 12 digits, then the length is specified by the hexadecimal value C as shown in Table 5–1.

Table 5–1: PIN Length Hexadecimal Equivalent

PIN Length	Hexadecimal Equivalent
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C

Format 0 PIN Block is used to build a PIN block from two strings that consist of 16 hexadecimal digits each. These strings are formed from the PIN, PIN length, certain PAN digits, and pad characters. The XOR operation described in Appendix C is used to create the PIN block from the two strings.

1. Build STRING-1 as follows:
   a. Zero-fill the first position.
   b. Enter the PIN length (one of the hexadecimal values from Table 5–1) in the second position.
   c. Enter the PIN beginning in the third position.
   d. Pad the remaining positions with hexadecimal Fs.
2. Build STRING-2 as follows:
   a. Zero-fill the first four positions.

b. Enter the right-most 12 digits of the PAN (excluding the account number check digit) in the remaining positions.

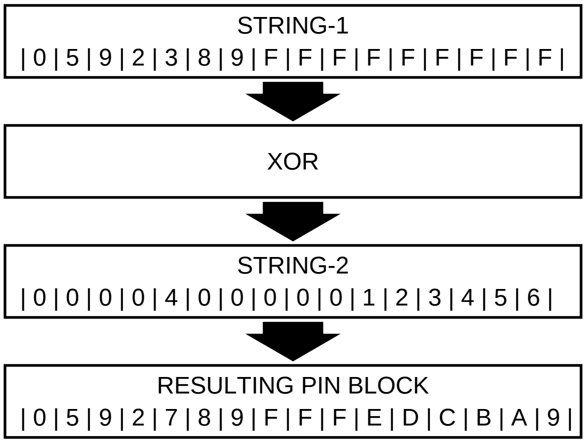
Account #4000 001 456 900 = 0000 4000 0014 5690

Account #4000 0012 3456 9002 = 0000 0001 2345 6900

3. Combine STRING-1 and STRING-2 through the XOR operation.

The following Format 0 PIN Block is built from PAN 4000001234569002 and PIN 92389, as shown in Figure 5–3:

Figure 5–3: String-1 XORed With String-2 to Calculate PIN Block Format 0


STRING-1
| 0 | 5 | 9 | 2 | 3 | 8 | 9 | F | F | F | F | F | F | F | F | F |
XOR
STRING-2
| 0 | 0 | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
RESULTING PIN BLOCK
| 0 | 5 | 9 | 2 | 7 | 8 | 9 | F | F | F | E | D | C | B | A | 9 |

5.2.2 ISO Format 3 PIN Block

The Format 3 PIN block is the same as the Format 0 PIN Block except for the fill digits. In ISO Format 3, the fill digit is a 4-bit field, with values from 1010 (10) to 1111 (15), where the fill-digit values are randomly or sequentially selected from this set of six possible values, such that it is highly unlikely that the identical configuration of fill digits will be used more than once with the same account number field by the same PIN encipherment device.

5.2.3 ISO PIN Block Format 2

The Format 2 PIN Block must be used for PINs that are submitted from the chip card reader to the chip on the card. This applies whether the PIN is submitted in plain text or enciphered using an encipherment key of the chip on the card. PINs enciphered only for transmission between the PIN entry device and the chip card reader shall use one of the PIN block formats specified in ISO 9564-1, with the exception of the Format 2 PIN block.

The Format 2 PIN Block is formed by the concatenation of two fields: the plain text PIN field and the filler field as defined in ISO 9564-3.

5.3 Network Security Techniques

Visa recognizes that cryptographic network security is an evolving technology. A growth path must be provided to accommodate different network security techniques as they become available. Possible network security enhancements include:

- Message Authentication Codes (MACs) to protect data against unauthorized change.
- Variable data elements, such as time stamps and transaction trace numbers, to match a request explicitly with a response.
- Alternate encryption procedures and key management techniques.

5.3.1 Security Format Code

To accommodate and distinguish between different network security techniques, each technique is identified by a unique, two-digit Security Format Code. When network users employ different techniques, the network will perform all the necessary translations between the source and destination techniques.

The Security Format Code allows migration to new network security techniques and eliminates the need for a simultaneous, systemwide change to implement new techniques.

Zone encryption is the only security technique currently supported. The Security Format Code assigned to this technique is 20, which indicates that zone encryption is the network security method and that the PIN is the only data element that must be encrypted.

5.3.2 Zone Encryption

Zone encryption is a DES-based technique that divides a network into different encryption zones (see Figure 5–4). A zone is characterized by the following elements:

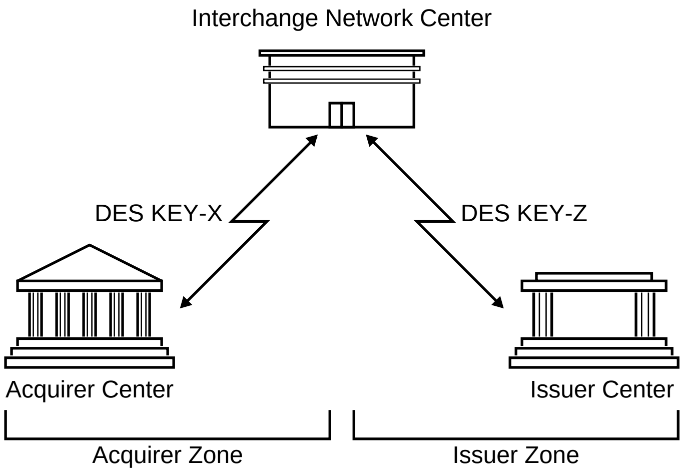
- Unique Zone Keys—Within each zone, a secret DES key is used to encrypt PINs in interchange messages. The DES key used must be unique to that zone.
- Interchange Keys—The DES key used to encrypt outgoing interchange PINs must be reserved for interchange use.
- Start of Zone—A zone begins in the machine that encrypts a PIN in that zone’s DES key and continues on through the facilities used to transmit the encrypted PIN.
- End of Zone—A zone ends when the encrypted PIN reaches its destination or when the PIN is no longer encrypted under that zone’s key.

- Physical Security—A zone starts and ends at a physically secure device.

NOTE: *The termination point of an issuer zone is an exception to this requirement. Because the issuer's endpoint handles only an issuer's PINs and is under the issuer's control, physical security can be maintained using the issuer's methodology.*

From a security perspective, a communications network is divided into acquirer zones and issuer zones. Between acquirers and issuers, the network operates an interchange network center through which all interchange messages pass as shown in Figure 5–4.

Figure 5–4: Network Using Zone Encryption



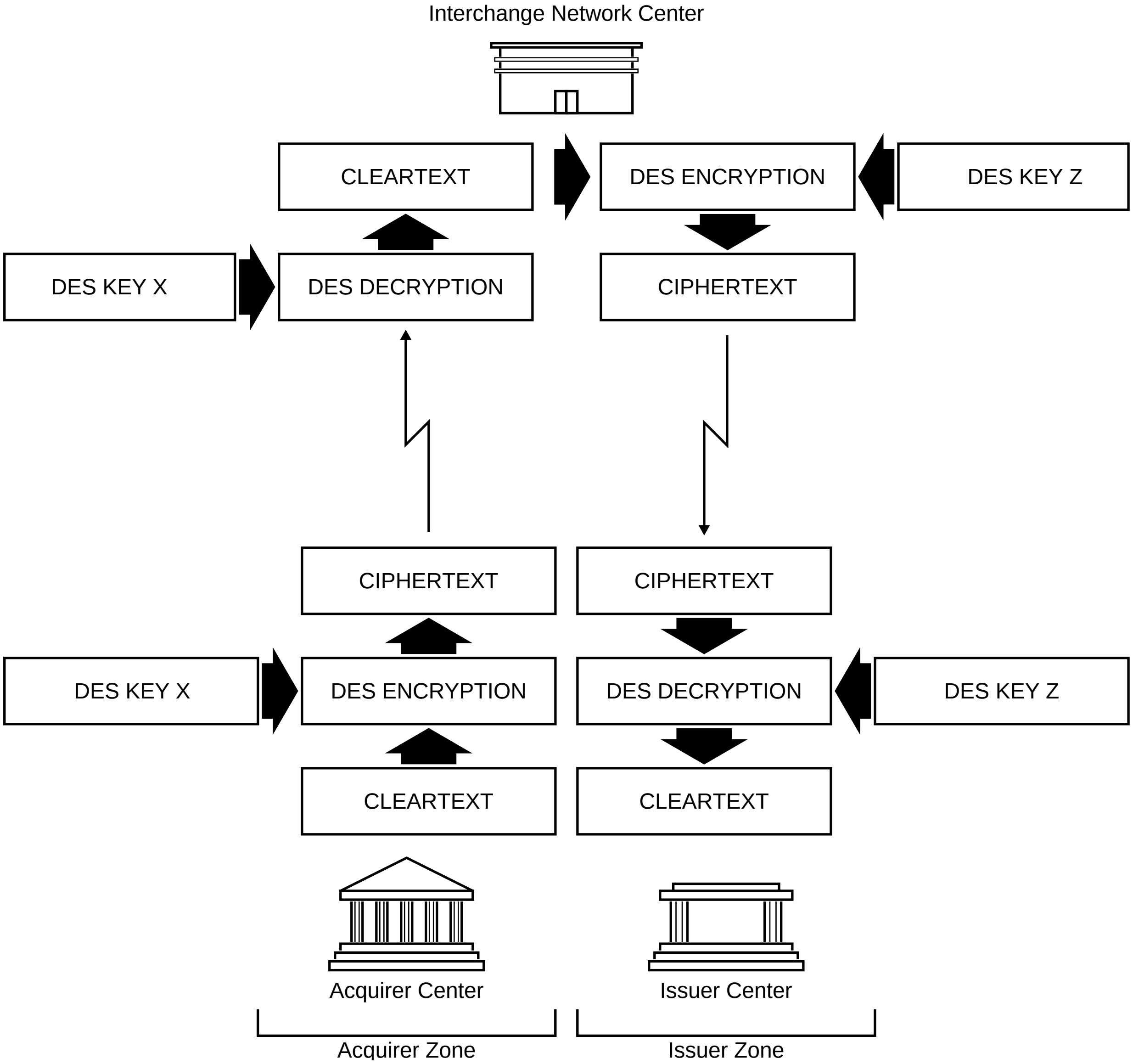
To ensure security, a PIN in an interchange message follows the path described here and illustrated in Figure 5–5.

1. In a physically secure device, the acquirer uses KEY-X to encrypt the PIN.
2. The encrypted PIN is transmitted through the acquirer zone to the interchange network center.
3. In a physically secure device, the interchange network center performs a PIN translation. The translation process uses KEY-X to decrypt the incoming PIN and then re-encrypts the PIN using KEY-Z (the issuer's DES key).
4. The interchange network center sends the encrypted PIN through the issuer's zone to the issuer.
5. The issuer uses its key to decrypt the PIN.

The security of zone encryption, as well as the ability to change the DES key for a given zone without affecting other zones, depends on each zone using a different, unique DES key. This requirement applies to all acquirer and issuer zones, even if an acquirer zone and issuer zone are both associated with the same network user.

NOTE: *A zone can begin in an automated teller machine (ATM) or in an encrypting PIN pad and end in a physically secure device at the acquirer's processing center. The acquirer's physically secure device must then translate the PIN from the ATM or PIN pad key to the key of the acquirer-to-interchange network center zone.*

Figure 5–5: Interchange Message Path



PIN Verification Method 6

A PIN must be verified at the issuer's processing center or by a designated agent. In the VisaNet Integrated Payment (V.I.P.) System, Visa may act as an issuer's agent by providing the PIN Verification Service (PVS). This service compares the cardholder's PIN entry to a cryptographic transformation of that PIN. This technique is referred to as the PIN Verification Value (PVV) method of verification.

This chapter describes the PVV verification method. Visa does not require the use of PVVs or the PVV method unless an issuer elects to use the PVS.

6.1 Process Overview

The PVV method is a two-step process.

1. When a card is issued, the issuer derives a 4-digit PVV. The PVV and PIN Verification Key Index (PVKI) are encoded on the magnetic stripe of the card or in an online database. The stored PVV is called the reference PVV for comparison.
2. When a cardholder enters a PIN, a transaction PVV is generated. The *transaction PVV* is then compared to the *reference PVV* by the issuer's processing center or agent. If the two PVVs match, there is a high probability (9999 in 10,000) that the PIN is correct.

The PVV method is described in detail in the next sections.

6.2 Limitations

PVVs are four-digit decimal values. For any one PVV, there are only 10,000 possible combinations of digits. If an adversary has a method of trying all 10,000 PVV combinations on a single account, the adversary will discover the PIN (or an equivalent value that transforms to the same PVV).

It is not feasible to test all 10,000 combinations manually. However, it may be possible to obtain the information needed to perpetrate a fraud by using an automated method (such as inserting minicomputers in communication lines, creating spurious transactions, and recording authorization responses).

Automated testing trials such as these would not expose the PIN Verification keys but could compromise an individual PIN/PAN combination. To detect such trials, the PIN Verification Service monitors the entry of incorrect PINs and declines transactions when the maximum number of incorrect PINs has been entered. Refer to the *V.I.P. System BASE I Processing Specifications*, *V.I.P. System SMS POS Processing Specifications* and *V.I.P. System SMS ATM Processing Specifications* manuals for detailed descriptions of this service.

6.3 Algorithm and Keys

The PVV method is based on the Data Encryption Standard (DES) algorithm and a pair of DES keys designated as a PVK pair. The algorithm may be implemented in hardware or software within a tamper-resistant security module.

Each issuer creates its own PVKs. These keys should be different from any other DES keys used by that issuer. Because each issuer has unique keys, a breach of security is limited to a particular issuer rather than to all issuers using the PVV method.

To create a PVV, the PVK pair is input to the DES algorithm together with other data. Like any DES-based scheme, the security depends on the secrecy of the DES keys.

The PVK pair must be kept secret and should not be known to anyone. If the unauthorized disclosure of a PVK pair is known or suspected, the PVK pair should be immediately replaced. Cards with PVVs generated using the potentially compromised key should be reissued as soon as possible, and when all such cards have been reissued, the potentially compromised PVK pair should be invalidated. To minimize the number of cards that should be reissued under this condition, it may be desirable to use a new PVK pair for each reissue.

Alternatively, a file of PVVs can be generated and sent to Visa. This file of PVVs takes priority over a PVV encoded on a card.

Visa allows up to six sets of PVKs. Procedures to generate and manage PVKs are presented in Chapter 7, DES Key Management.

6.4 Data Elements

The following data elements are required to generate a PVV:

- Primary Account Number (PAN)

- PIN associated with the PAN
- 1-digit PIN Verification Key Index (PVKI)
- A PVK pair Card Technology Standards Manual Data Element

6.4.1 PAN Digits

The right-most 11 digits of the PAN, excluding the modulus-10 check digit, are used to generate the PVV. See Table 6–1 for an example.

Table 6–1: Example of PAN Digit Selection for PVV Generation

PAN	PAN Digit Selection
4839 1234 5678 9019	1234 5678 901

6.4.2 PIN Digits

The PIN associated with the PAN is used to generate the PVV. The digits used are selected according to PIN length.

When the PIN is four digits, the entire PIN is used to generate the PVV.

When the PIN has more than four digits, only the left-most four digits are used to generate the PVV.

6.4.3 PIN Verification Key Index (PVKI)

The PVKI is a 1-digit value that identifies which pair of keys is to be used for the PVV computation. The PVKI is encoded on the magnetic stripe as part of the PIN Verification field or stored in an online database.

A PVKI can be any value between zero and six.

A zero indicates that the PIN cannot be verified through the PIN Verification Service (PVS). If the issuer specified to Visa that the PVS is to be performed by Visa for a specified account range, and an individual card has a PVKI of zero, Visa will decline transactions with PINs for that card. If the PVKI is zero, the PVV need not be generated unless the issuer elects to do so for on-us transaction use.

A PVKI value between 1 and 6 identifies the appropriate PVK pair.

6.4.4 PIN Verification Key (PVK) Pair

The PVK pair consists of two odd-parity DES keys. The two keys should not be identical. Greater security is provided when each key is a unique value.

Refer to Chapter 7, DES Key Management, for standards and guidelines covering the generation and management of PIN Verification Keys.

NOTE: *It is recommended that an issuer hold at least one PVK pair in reserve for activation in the event of a known security breach.*

6.5 Computing the PVV

The following guidelines should be observed during the PVV computation process:

- All processing should take place on a physically secure device.
- No computer printout of PIN/PAN combinations should be generated except under highly controlled conditions. Any printout needed for checking purposes should be destroyed after the verification process is finished.
- Senior management should closely supervise the entire PVV computation process.

The PVV computation process consists of the following steps:

1. Build a 64-bit Transformed Security Parameter (TSP) from the PAN, PIN, and PVKI.
2. Execute the DES algorithm on the TSP and the PVK pair.
3. Select four numeric digits as the PVV from the resulting ciphertext.

Each of these steps is described below.

6.5.1 Building a Transformed Security Parameter (TSP)

A TSP is built according to the specifications in Table 6–2. The resulting 64-bit TSP is equivalent to a string of 16, 4-bit hexadecimal characters.

Table 6–2: Structure of Transformed Security Parameter (TSP)

Position	Length	Contents
1–11	11	PAN—the 11 right-most digits of the cardholder’s account number excluding the mod-10 check digit
12	1	PIN Verification Key Index

Table 6–2: Structure of Transformed Security Parameter (TSP)

Position	Length	Contents
13–16	4	4-digit PIN or left-most four digits of a longer PIN

The ensuing TSP example contains the following assumptions:

- PAN = 4839 1234 5678 9019
- PVKI = 3
- PIN = 387283

  TSP = 1234567890133872

6.5.2 Executing the DES Algorithm

The DES algorithm is executed on the TSP and PVK pair as described in the following procedure. The result is a 64-bit block of ciphertext equivalent to 16 hexadecimal characters called the encrypted TSP.

6.5.2.1 Preparation

1. Obtain the PVK pair that corresponds to the PVKI specified in the TSP.
2. Designate one of the keys as PVK-A and the other as PVK-B.
3. If the PVK pair is encrypted under another key, decrypt each key in the pair.

6.5.2.2 Triple Encryption Procedure

Perform the following steps to triple-encrypt the TSP:

1. Set the DES function to encrypt. Encrypt the TSP under PVK-A.
2. Set the DES function to decrypt. Using PVK-B, decrypt the result of step 1.
3. Set the DES function to encrypt. Encrypt the result of step 2 under PKV-A.

6.6 Selecting the PVV Digits

From the encrypted TSP, select the four decimal digits, as follows:

1. Scan the encrypted TSP block from left to right, skipping any digits greater than nine, until the four decimal digits are found. If the four decimal digits can be obtained from this scan, those digits are the PVV. The computation process is complete.
2. If, at the end of the scan, fewer than four decimal digits are selected, scan from left to right again, as follows:
   a. Scan only those digits greater than nine.
   b. Subtract 10 from the scanned digit.
   c. Select the result as a PVV digit.
   d. Continue the scan until all four PVV digits are selected.

Figure 6–1 illustrates the process for a single scan. Figure 6–2 illustrates a double-scan process.

Figure 6–1: Sample PVV Computation (Single Scan of the TSP)

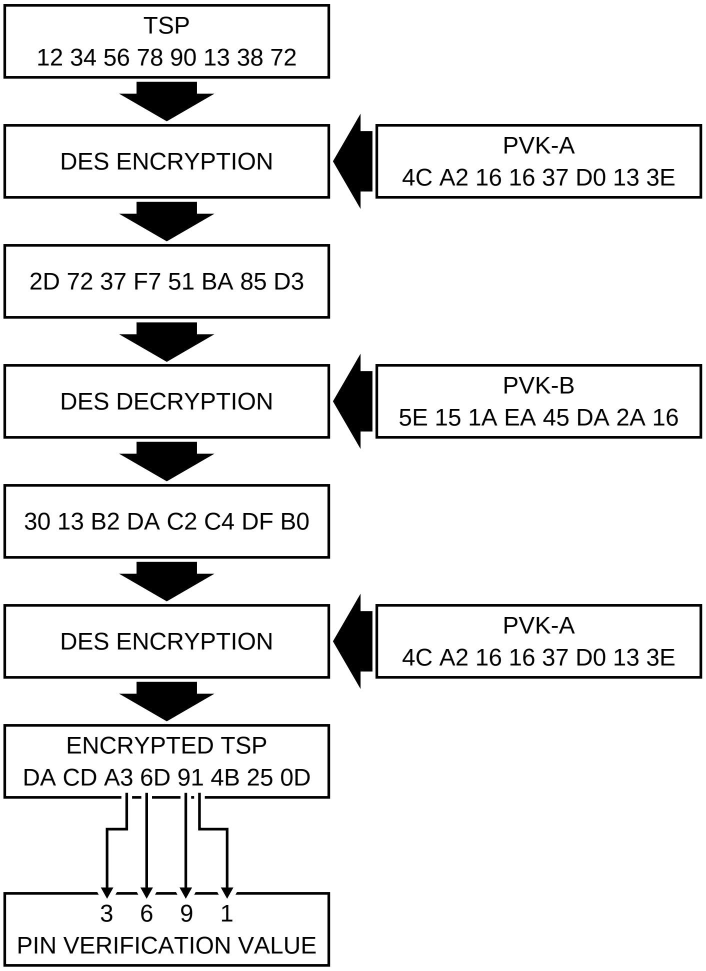
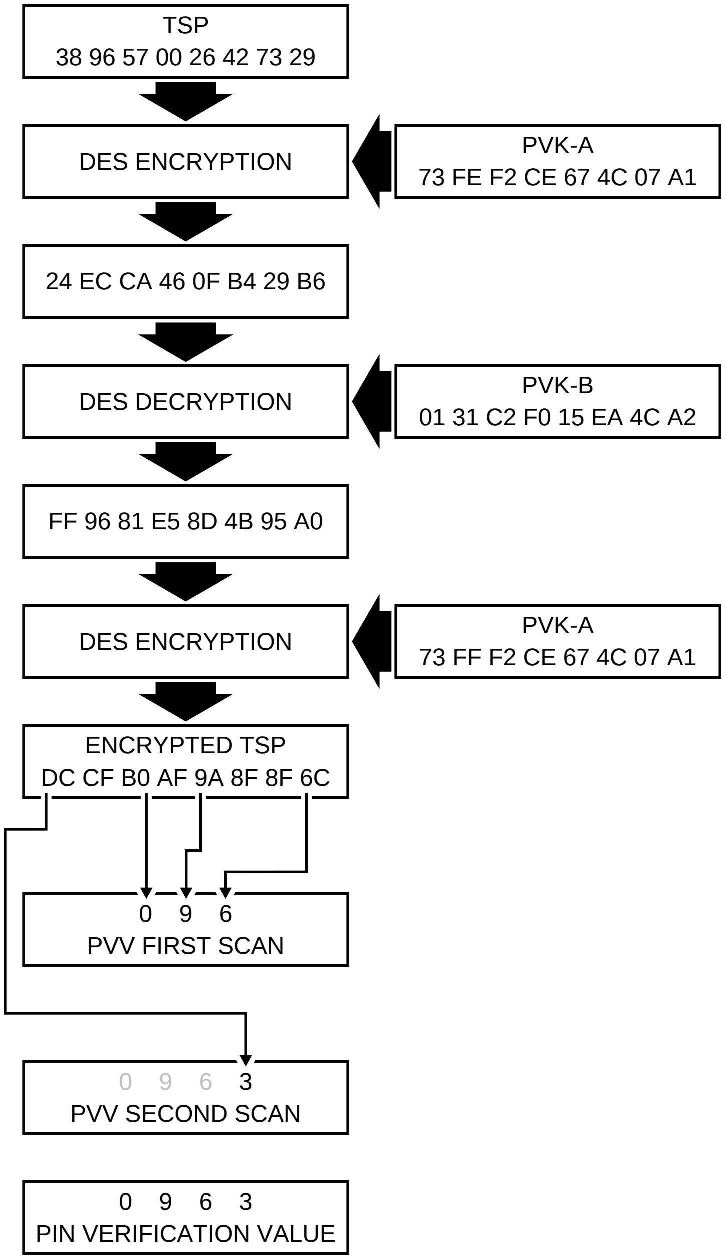


Figure 6–2: Sample PVV Computation (Double Scan of the Encrypted TSP)



6.7 IBM 3624 PIN Offset Processing

6.7.1 IBM 3624 PIN Block Format

The IBM 3624 PIN Block Format supports a PIN from 1 to 16 digits in length. When the PIN has more than 16 digits, only the left-most 16 digits are used.

Figure 6–3 illustrates the IBM 3624 PIN Block Format.

Figure 6–3: IBM 3624 PIN Block Format

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
P	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X	P/X

P is a PIN digit, which is a 4-bit value from hexadecimal 0 to hexadecimal 9. The values of the PIN digits are independent.

P/X is a PIN digit or a pad value. A PIN digit has a 4-bit value from hexadecimal 0 to hexadecimal 9. A pad value has a 4-bit value from hexadecimal 0 to hexadecimal F and must be different from any PIN digit. The number of pad values for this format is in the range from 0 to 15 and all the pad values must have the same value.

The ensuing example contains the following assumptions:

- PIN = 0123456
- Pad = hexadecimal E

Resulting PIN block = X“0123456EEEEEEEEE” 1

NOTE: *The IBM PIN Block Format is not allowed to be used in any VisaNet interchange transactions.*

6.7.2 IBM 3624 PIN Calculation Method

The IBM 3624 PIN calculation method produces a PIN that is 4 to 16 digits in length. The calculation is performed as follows:

1. Encrypt the hexadecimal validation data with a key that has a control vector that specifies the PINGEN (or PINVER) key type to produce a 64-bit quantity.

2. Convert the character format decimalization table to an equivalent array of 16 (sixteen) 4-bit hexadecimal digits, and use the decimalization table to convert the hexadecimal digits (hexadecimal 0 to hexadecimal F) of the encrypted validation data to decimal digits (hexadecimal 0 to hexadecimal 9). Call this result *newpin*.

   Let *newpin(i), decimalizaion_table(i),* and *encrypted_validation_data*(i) each represent the (i)th hexadecimal digit in each quantity.

   The digits of newpin are obtained by the following procedure:

   ```
   For i = 1 to 16 do:
   j := encrypted_validation_data(i)
   newpin(i) := decimalization_table(j)
   end do
   ```

3. Select *n* left-most decimal digits of newpin, where *n* is the PIN length. The result is an n-digit calculation PIN. The PIN must be from 4 to 16 digits in length.

The example in Figure 6–4 is for a 6-digit PIN.

Figure 6–4: Example of IBM 3624 PIN Calculation Method

Encrypted Validation Data	=	E5C1BD67B66AE7C6
Decimalization Table Index	=	0123456789ABCDEF
Decimalization Table	=	8351296477461538
Newpin	=	3913656466643416
PIN Length	=	6
Calculated PIN (left-most 6 digits of newpin)	=	391365

6.7.3 IBM 3624 PIN Offset Calculation Method

The IBM 3624 PIN offset calculation method is the same as the IBM 3624 PIN calculation method, except that there is an additional step after the PIN is generated to generate or use an offset.

- To generate an offset, the additional step subtracts (digit-by-digit, modulo 10, with no carry) the generated PIN from the customer-selected PIN.

The result is a PIN offset of n decimal digits, where n is the PIN length and must be in the range of 4 to 16. The PIN_check_length parameter specifies n as the low-order (right-most) digits of the n-digit PIN offset. The PIN offset is not encrypted.

- To use an offset to verify a trial PIN, the additional step adds (digit-by-digit, module 10, with no carry) the offset to the generated PIN. The result is compared to the customer-entered trial PIN.

NOTE: *The digit-wise subtraction is defined only for digits in the range from X“0” to X“9”. No other value is valid and will cause processing to fail.*

The length of the offset depends on the length of the PIN and the length of the offset must be less than or equal to the length of the PIN. The financial institution that issues the magnetic stripe card determines the length of the PIN offset, which is specified with the PIN_check_length parameter.

When the length of the PIN offset is less than the length of the generated PIN, the subtraction or addition begins with the low-order PIN digit.

DES Key Management 7

The process of securely generating, distributing, and storing Data Encryption Standard (DES) keys is called *Key Management*. Key management procedures must be highly secure. The compromise of even a single key could lead to the compromise of all PINs (personal identification numbers) encrypted under that key.

The requirements in this chapter apply only to VisaNet interchange transactions. Members may process on-us transactions any way they choose.

In VisaNet interchange, a DES key has one of the following functions:

- A working key protects PINs and other data.
- A master key protects other keys.

7.1 Working Keys

Working keys are secret values that are input to the DES process. The following are examples of working keys:

- The keys needed to encrypt and decrypt PINs before and after message transmission or host storage.
- The pair of keys used to generate the PIN Verification Value (PVV).
- The pair of keys used to generate the Card Verification Value (CVV).
- The pair of keys used to generate the Card Authentication Verification Value (CAVV).
- The keys (up to 24 sets) used in Visa Smart Debit/Visa Smart Credit (VSDC) processing.[1]

To obtain valid results, the same working key must be used both for encryption and for decryption. Likewise, to verify a PIN with the PVV or to validate a CVV, the original encryption keys are required.

The following working keys are used to process VisaNet interchange transactions:

- Acquirer Working Key (AWK)—Used by an acquirer to encrypt PINs in outgoing interchange transactions. This key is also used by Visa for decryption during PIN translation.
- Issuer Working Key (IWK)—Used by Visa to encrypt PINs during PIN translation. This key is also used by the issuer to decrypt incoming interchange PINs.
- Cardholder Authentication Verification Value Key (CAVV)—Used during the Verified by Visa (VBV) process.

NOTE: *A member uses an AWK to protect outgoing PINs and an IWK to decipher incoming encrypted PINs.*

- PIN Verification Key (PVK) pair—Used to transform a PIN into a PIN Verification Value (refer to Chapter 6).
- Card Verification Key (CVK) pair—Used to generate and verify the Card Verification Value (CVV) that is encoded on both Track 1 and Track 2 of the magnetic stripe (refer to Chapter 2).
- Master Derivation Key (MDK)—Used for the VSDC cryptogram processing associated with card authentication, issuer authentication, and dispute processing.

[1] For additional information on Visa Smart Debit/Visa Smart Credit (VSDC), please refer to the *Visa ICC (Integrated Circuit Card) Specification, (VIS).*

7.1.1 Standards

The standards in Table 7–1 apply to all working keys (AWK, IWK, MDK, PVK pair, CVK pair, or CAVV pair) unless otherwise noted.

Table 7–1: Working Keys Standards (1 of 2)

Attribute	Standard
Number of Keys	• One AWK is required to send outgoing interchange PINs. • One IWK is required to receive incoming interchange PINs. • Two AWKs or two IWKs can be created to provide the member with the ability to change working keys in an orderly manner. The two keys also provide fall-back protection in case a key change is not successful. • At least one pair (up to six sets) of PVKs is required for issuers who use the PIN Verification Service. • A pair of CVKs (up to two sets) is used in the process to generate and verify that the CVV that is encoded on Track 1 and Track 2 of the magnetic stripe. • At least one pair (up to 24 sets) of MDKs. • At least one pair of CAVV keys is required for issuers who participate in Verified by Visa (3D Secure)
Ownership	Working keys are the property of the member. They may be generated by the member or by Visa (at the member's request). Working keys are controlled by the member.
Randomness	• For an AWK—A random process must be used to generate the AWK. Refer to the "Member Working Key Generation Procedures" section in this chapter for the procedure to generate a random key. • For an IWK, MDK, PVK pair, CVK pair, or CAVV pair generated by the member—An issuer may use any method considered suitable. Visa recommends that an issuer observe the same standard as for acquirers.
Disclosure	• For an AWK—Visa mandates the use of a physically secure device and recommends the use of completely automated procedures to maintain the security of the AWK. The AWK should not be known to, or be accessible by, anyone. • For an IWK, MDK, PVK pair, or CVK pair, or CAVV pair—Visa strongly recommends that issuers use the same degree of security with these keys as is required for AWKs.

Table 7–1: Working Keys Standards (2 of 2)

Attribute	Standard
Other Uses	• For an AWK—The AWK must not be used for any purpose other than to provide cryptographic security between the member and Visa. • For an IWK, MDK, PVK pair, CVK pair, or CAVV pair—Visa strongly recommends the use of unique, reserved values for the IWK, MDK, for each key of the PVK pair, and for each key of the CVK pair, or CAVV pair.
In-House Storage	• For an AWK—When an AWK is stored outside a physically secure device, it must be encrypted under a member master key. The member master key must be protected at all times and can reside only within a physically secure device. • For an IWK, MDK, PVK pair, or CVK pair, or CAVV pair—The issuer may store these keys in any manner considered suitable. For greater security, Visa strongly recommends that an issuer observe the standard for an AWK. • Members should have encrypted backup key copies as Visa does not re-send keys.
Conveyance	• To a member—At a member's request, Visa will generate one, some, or all working keys for the member (AWK, IWK, MDK, PVK pair, CVK pair, CAVV pair). When Visa-generated keys are mailed to a member, they are encrypted under that member's ZCMK. The procedure for a member to ask Visa to generate keys is explained in "Creation and Conveyance Procedures." • To Visa—Any key sent to Visa must be encrypted under the member's ZCMK. A key check value must accompany each AWK, IWK, MDK, PVK pair, or CVK pair, or CAVV pair sent to Visa. The MDK requires a double-length conveyance key.

7.1.2 Creation and Conveyance Procedures

After the ZCMK is established and confirmed by Visa, the working keys can be created and conveyed. Keys can be created by the member or Visa. In either case, the keys must then be conveyed from the creator to the other party.

If Visa will create the working keys and convey them to the member, see the section, "Visa Working Key Creation Procedure" later in this chapter. If the member will create its own working keys and convey them to Visa, see the "Member Working Key Creation Procedure" section.

7.1.2.1 Visa Working Key Creation Procedure

The Visa Working Key Creation procedure can be used to create

- An entire set of working keys (AWK, CAVV, IWK, MDK, PVK pair, and CVK pair).
- Any single key or key pair.
- Any combination of keys, key pairs, or both.

Visa will create working keys at a member's request any time following a member's confirmation of ZCMK generation. The member can ask for key creation in conjunction with the ZCMK creation request or after the ZCMK creation request.

The procedure in Table 7–2 explains how a member authorizes Visa to create its working keys and how Visa conveys the keys to the member once they are created. The forms used in this procedure are located in Appendix D.

Table 7–2: Visa Working Keys Creation Procedure (1 of 2)

Responsible Party	Action
Member	1. Copies the Visa Key Management Request Form. 2. Completes the requestor identification and authorization section and enters the Activation Date for Key. or If this request is made in conjunction with a ZCMK creation request, completes steps 1 and 2 of the ZCMK Creation Procedure and attaches the completed Designation of Key Custodians Form to the Visa Key Management Request Form. 3. Performs the following activities in the working keys section: a. Completes the ZCMK Creation Date field. b. Completes the ZCMK Key Check Value field. c. Specifies the reason for this working key creation request: Original, Replacement, or Additional. d. Places a check by Create the Following Working Keys. e. Specifies the number of keys being requested in the brackets to the left of the type of working keys being requested. f. If replacement keys are being requested, enters the indexes of the keys on the lines to the right of the type of working keys being requested. (Not applicable for MDKs.) 4. If requesting MDKs, completes the Key Conveyance Form for Master Derivation Key. For original and additional requests, completes the Derivation Key Index (DKI) field. The DKI must be a unique number from 1 to 255. Places a check by Online UDK (Unique Derivation Key) single-length or double-length if Visa is performing authentication processing on behalf of the member. For replacement requests, completes the Replaces DKI field identifying the DKI being replaced, completes the DKI field for the new DKI, and places a check by Online UDK single-length or double-length if appropriate. If only the DKI is being replaced (rather than the entire key information), the member must indicate not applicable (n/a) as the MDK value on the form. 5. Send the completed form(s) by courier to its Member Services representative at Visa.

Table 7–2: Visa Working Keys Creation Procedure (2 of 2)

Responsible Party	Action
Visa	1. Creates the requested working keys and encrypts them using the member's ZCMK. If working keys are requested when the ZCMK is requested, the creation of the working keys is delayed until the ZCMK is combined, confirmed, and conveyed to Visa. 2. Prints the encrypted keys, their creation date and time, and their key check values. Mails that printout to the member for storage.
Member	When the keys are received, decrypts them using the ZCMK and encrypts them again using a member master key.

7.2 Key Exchange Keys

Key Exchange Keys (KEKs) are used to protect (in other words, encrypt and decrypt) working keys so they can be safely stored or conveyed from one network node to another.

The Zone Control Master Key (ZCMK) is a type of KEK. It is used to protect the AWK, CAVV, IWK, MDK, PVK pair, and CVK pair during transit. The sole purpose of the ZCMK is to protect working keys so that they can be sent safely to Visa and the member.

A member uses the ZCMK to encrypt working keys before sending them to Visa. Visa uses the ZCMK to decrypt the working keys it receives. Before storing the member's keys, Visa encrypts them again under a key known only to Visa.

Visa uses the ZCMK to encrypt working keys before sending them to a member. A member uses the ZCMK to decrypt the working keys it receives.

7.3 Master Keys

A member master key is used by a member to protect its keys for in-house storage. This key is known only within a physically secure device at the member's processing center. For example, a member master key could be used to encrypt any of the working keys, KEKs, or ZCMKs used in interchange processing. The same member master key should not be used to encrypt both working keys and master keys.

7.4 Zone Control Master Key (ZCMK)

The following standards apply to the Zone Control Master Key (ZCMK).

7.4.1 Standards

Table 7–3 describes the standards that apply only to the ZCMK..

Table 7–3: ZCMK Standards

Attribute	Description
Number of Keys	Each member uses a ZCMK that protects the member's working keys during conveyance to and from Visa. A member may have more than one ZCMK.
Ownership	A ZCMK is the property of the member that uses it. A ZCMK is generated by Visa and controlled by the member.
Generation	Visa uses a secure process to generate the ZCMK. It is sent to the member in three separate, cleartext component parts with a ZCMK key check value.
Valid Use	The ZCMK must be reserved exclusively to encrypt working keys for conveyance to Visa and cannot be used for any other purpose.
In-House Storage	**By an acquirer**—When the ZCMK is stored by the acquirer outside a physically secure machine, it must be encrypted under a member master key. The member master key must be protected at all times and can reside only within a physically secure machine. Visa requires that the three cleartext components be destroyed once the ZCMK is encrypted under a member master key. **By an issuer**—This requirement does not apply to an issuing-only member. However, Visa recommends that an issuer observe this standard for greater security.
Conveyance	Visa conveys the three ZCMK components and a key check value for the ZCMK to the member as described in the following section "Creation Process".

7.4.2 Creation Process

A ZCMK is created from three ZCMK components. Keys may be double-length or single-length. Each component has the characteristics of a DES key as follows:

- The double-length component consists of 32 hexadecimal characters. The single-length component consists of 16 hexadecimal characters.
- Each pair of hexadecimal characters (byte) is adjusted for odd parity. The least significant bit (right most) is the parity bit.
- The component is generated using a random process so that the resulting value is unpredictable.

The ZCMK is created by combining the three cleartext components through a mathematical operation known as exclusive-OR (XOR), which is described in Appendix C.

The member initiates the creation process by sending a request to Visa. Visa creates a new ZCMK in the form of three cleartext components. The member combines its ZCMK upon receipt of the components. The following sections detail the ZCMK creation process. Note that the ZCMK itself is never conveyed. The forms used in this procedure are contained in Appendix D.

Note that the ZCMK itself is never conveyed.

7.4.2.1 Member Requests ZCMK Creation

The member requests ZCMK creation, as follows:

1. The member copies the Visa Key Management Request Form and then:
    a. Completes the requestor identification and authorization section
    b. Enters the Activation Date for Keys
    c. Checks single or double (indicating the key length) in the “Create a New ZCMK” section
2. The member copies the Designation of Key Custodians Form.
3. The member identifies three employees who are to receive and have control of the three ZCMK components. Key custodians must be made aware of their responsibilities. The following information represents the “best practices” relative to the selection and role of the three key custodians:

- The individuals chosen to perform the functions of the key custodian are to be “trusted” employees. The classification of a trusted employee is typically at the discretion of the member, but it generally does not include temporary help, new employees, or employees that have a “probationary” status.
- The designated key custodians should not be in the same line of management. Specifically, there should be no situation where two of the key custodians report to the third. It is strongly recommended that the three custodians be appointed from different functional areas (for example, operations, data security, and internal audit).

At the discretion of the member’s management, a second set of alternate or “back up” individuals may also be identified to perform the primary custodians’ responsibilities when the latter are not available. These statements also apply when selecting alternates.

NOTE: *Requirements applicable to the management ZCMK’s are stated in the* PIN Security Requirements *manual*

4. The member completes the Requestor Identification section and then records the names, titles, and addresses of those three employees.
5. The member forwards both completed forms to its Member Services Representative at Visa.

7.4.2.2 Visa Responsibility for ZCMK Creation

After receiving a member request for ZCMK creation, Visa:

1. Verifies authenticity of Key Request Form.
2. Creates three ZCMK cleartext components and their key check values and the key check value for the new ZCMK.
3. Creates three ZCMK component mailers. Each tamper-evident security envelope contains one of the ZCMK cleartext components and the key check value for that component. The key check value for the new ZCMK generated from all three components is included in each of the three mailers.
4. Ships one component mailer to each of the designated recipients using different express mail carriers and staggered over different business days.

7.4.2.3 Member Responsibilities After Receiving ZCMK Components

After receiving the express mail package containing the ZCMK components, the responsible key custodian (and the designated alternate, if one has been selected), performs the following activities:

1. Examines the external envelope for signs of tampering. Immediately report any suspicions of tampering to the member's internal security department and to Visa.

2. Opens the mailing envelope and removes the contents.

3. Examines the security envelope containing the key component data for signs of tampering. Immediately reports any suspicions of tampering to the member's internal security department and to Visa. Do not open the security envelope until directed to do so.

4. Stores the unopened security envelope in a locked security container that is only accessible by the key custodian or by the designated alternate.

5. The member should contact their Visa Member Services representative by email, acknowledging receipt of their three ZCMK components. If Visa does not receive such an acknowledgement within 10 business days after the last key component was mailed, the key will be invalidated and the process will start over.

6. Create an access log to record the receipt of the key component from Visa. The member's internal audit department can use the log to verify compliance with the member's security standards for management of this (and other) cryptographic keys used in the card personalization process. Also, use the log to record every time the component is removed from the security container. The key custodian should record the purpose of the key component's removal, the time it was removed, and the time it was returned to the security container. The key custodian should sign the log for authentication.

7.4.2.4 Member Combines ZCMK Components

After receiving the ZCMK components, the member combines the components as follows:

1. In an automated environment, the member uses the XOR operation to combine the three ZCMK components. (Appendix C of this manual explains the XOR operation.)

   NOTE: *Visa requires the use of a physically secure device to perform the XOR operation.*

2. The member creates a key check value for the ZCMK. (Figure 7–3 illustrates the generation of a key check value.)

3. The member compares the generated key check value to the one provided by Visa.

- If the key check values match, the ZCMK has been created properly. Notify Visa.
- If the key check values do not match, notify Visa.

4. Once the key check values match, the member encrypts the ZCMK using the member's double-length master key in a secure, automated environment and then stores the encrypted ZCMK.

7.4.2.5 ZCMK Components Destruction

After verifying that the ZCMK has been correctly installed and is functional, the three key custodians are to destroy the ZCMK components. Destroy the key components, as follows:

1. Create a Key Component Destruction Form, which functions as an affidavit that the key component has been destroyed. The form should be signed by the designated key custodian (the alternate key custodian if used) and a representative from the member's data security or internal audit department.
2. Remove the key component from secure storage. Document in the log that the component is being removed so that it may be destroyed.
3. Take the component to a secure area where it may be shredded, burned, or destroyed by some method that renders the key component data unrecoverable.
4. The destruction must be witnessed by a non-key custodian such as a representative from the member's internal audit department.
5. All parties to the destruction process must verify the destruction of the component by signing the Key Component Destruction Form.
6. Store the Key Component Destruction Form in the security container for verification by the member's internal audit department.

IMPORTANT

> *Under no circumstances should the ZCMK components be saved after the ZCMK is generated and verified.*

If it is necessary to replace the ZCMK, the entire creation process must be repeated. When the replacement ZCMK has been installed at Visa, all keys conveyed to Visa thereafter must be encrypted using the replacement ZCMK.

NOTE: *The components should not be destroyed until AFTER the key check value has been used to validate the key.*

7.4.2.6 Member Working Key Creation Procedure

After the ZCMK is generated and confirmed, a member that elects to generate its own working keys can create those keys and convey them to Visa for installation in VisaNet. Table 7–4 explains this process. The forms used in this procedure are in Appendix D.

Table 7–4: Member Working Key Creation Procedure (1 of 2)

Responsible Party	Action
Member	1. Creates each working key and adjusts it for odd parity. Key generation and parity adjustment are discussed in the “Member Working Key Generation Procedures” section. 2. Calculates a key check value for each working key. (Figure 7–3 illustrates this process.) 3. Encrypts each working key under the ZCMK. 4. Copies the appropriate Key Conveyance forms. 5. Completes the Requestor Identification section and records each encrypted key with its key check value. ***Note:*** *Some of the forms have spaces for multiple working keys that depend on specific zone key indexes and PVKIs. Be sure to record keys in the appropriate area of the form.* For MDKs, there are specific guidelines: – For original and additional MDKs, completes the Derivation Key Index (DKI) field. The DKI must be a unique number from 1 to 255. Places a check by Online UDK (Unique Derivation Key) single-length or double-length if Visa is performing authentication processing on behalf of the member. – For replacement MDKs, completes the Replaces DKI field identifying the DKI being replaced, completes the DKI field for the new DKI, and places a check by Online UDK single-length or double-length if appropriate. If only the DKI is being replaced (rather than the entire key information), the member must indicate not applicable (n/a) as the MDK value on the form.

Table 7–4: Member Working Key Creation Procedure (2 of 2)

Responsible Party	Action
	6. Copies the Visa Key Management Request Form. 7. Completes the Requestor Identification and Authorization sections and enters the Activation Date for Keys. 8. Performs the following activities in the “Working Keys” section: a. Completes the ZCMK Creation Date field. b. Completes the ZCMK Key Check Value field. c. Specifies the reason for the key management request: Original, Replacement, or Additional. d. Places a check by Translate the Following Working Keys. e. Specifies the number of keys being conveyed to Visa in the brackets to the left of the type of working keys being sent. 9. Mails the Visa Key Management Request Form and Key Conveyance Form to its Member Services representative at Visa.
Visa	1. Upon receipt of the working keys, does the following: a. Translates each working key using the member's ZCMK. b. For each key, calculates the key check value and compares it to the key check value provided by the member. 2. Contacts the member to confirm that the keys are valid and to confirm the effective date for their use.

7.4.2.7 Member Working Key Generation Procedures

If a member elects to generate its own working keys, it may generate the DES keys using one of two methods:

- The key generation capability of a hardware security module
- A random number generator

NOTE: *Manual processes, such as the flipping of a fair coin, that results in random outcomes may be used. Most random number generation programs are not random enough for working key generation.*

If a random number generator is used, the following procedure applies:

1. Generate 64 random bits. These programs generate a value between zero and one. Each value must be either rounded down to zero or up to one. The result is used as one of the bits in the key.
2. Starting from the left-most bit, adjust every eighth bit (such as bits 8, 16, 24, and so on) as needed to obtain odd parity.

A manual key-generation process uses a coin toss to obtain a string of zeros and ones. These bits are developed in groups of four, then converted to hexadecimal characters.

1. Toss a coin. Write down a *zero* for tails and a *one* for heads. Repeat this process four times, until a four digit string is built (such as 1011).
2. Convert the four-digit string into its hexadecimal equivalent using Figure 7–1 (1011 = B).
3. Repeat steps 1 and 2 until 16 hexadecimal characters are created.
4. Write down the 16 hexadecimal digits in pairs.
5. Adjust the parity of each pair using Figure 7–2:
   - Initial value: A0 56 7D 9F 71 E3 12 0B
   - Adjusted value: A1 57 7C 9E 70 E3 13 0B
   - No adjustment is needed for a pair that is not included in Figure 7–2.

Figure 7–1: Binary to Hexadecimal Conversion

Binary = Hexadecimal	Binary = Hexadecimal
0000 = 0	1000 = 8
0001 = 1	1001 = 9
0010 = 2	1010 = A
0011 = 3	1011 = B
0100 = 4	1100 = C
0101 = 5	1101 = D
0110 = 6	1110 = E
0111 = 7	1111 = F

Figure 7–2: Parity Adjustment Table

Initial		Adjusted	Initial		Adjusted	Initial		Adjusted	Initial		Adjusted
00	→	01	41	→	40	81	→	80	C0	→	C1
03	→	02	42	→	43	82	→	83	C3	→	C2
05	→	04	44	→	45	84	→	85	C5	→	C4
06	→	07	47	→	46	87	→	86	C6	→	C7
09	→	08	48	→	49	88	→	89	C9	→	C8
0A	→	0B	4B	→	4A	8B	→	8A	CA	→	CB
0C	→	0D	4D	→	4C	8D	→	8C	CC	→	CD
0F	→	0E	4E	→	4F	8E	→	8F	CF	→	CE
11	→	10	50	→	51	90	→	91	D1	→	D0
12	→	13	53	→	52	93	→	92	D2	→	D3
14	→	15	55	→	54	95	→	94	D4	→	D5
17	→	16	56	→	57	96	→	97	D7	→	D6
18	→	19	59	→	58	99	→	98	D8	→	D9
1B	→	1A	5A	→	5B	9A	→	9B	DB	→	DA
1D	→	1C	5C	→	5D	9C	→	9D	DD	→	DC
1E	→	1F	5F	→	5E	9F	→	9E	DE	→	DF
21	→	20	60	→	61	A0	→	A1	E1	→	E0
22	→	23	63	→	62	A3	→	A2	E2	→	E3
24	→	25	65	→	64	A5	→	A4	E4	→	E5
27	→	26	66	→	67	A6	→	A7	E7	→	E6
28	→	29	69	→	68	A9	→	A8	E8	→	E9
2B	→	2A	6A	→	6B	AA	→	AB	EB	→	EA
2D	→	2C	6C	→	6D	AC	→	AD	ED	→	EC
2E	→	2F	6F	→	6E	AF	→	AE	EE	→	EF
30	→	31	71	→	70	B1	→	B0	F0	→	F1
33	→	32	72	→	73	B2	→	B3	F3	→	F2
35	→	34	74	→	75	B4	→	B5	F5	→	F4
36	→	37	77	→	76	B7	→	B6	F6	→	F7
39	→	38	78	→	79	B8	→	B9	F9	→	F8
3A	→	3B	7B	→	7A	BB	→	BA	FA	→	FB
3C	→	3D	7D	→	7C	BD	→	BC	FC	→	FD
3F	→	3E	7E	→	7F	BE	→	BF	FF	→	FE

7.5 Key Check Value

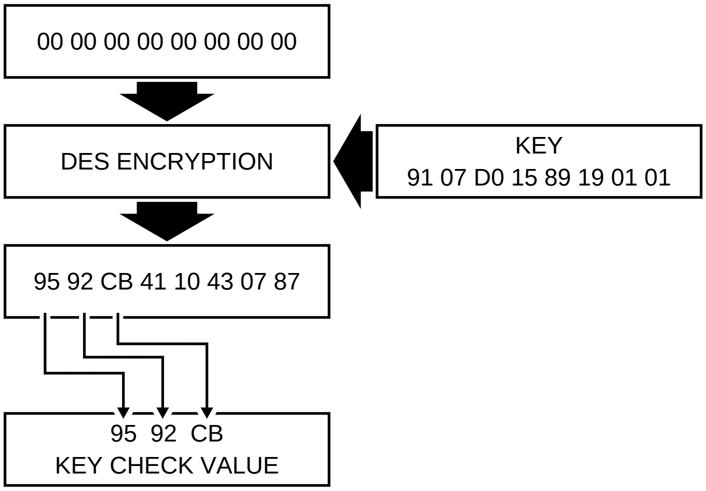
A key check value is a six-digit, hexadecimal value that is obtained by encrypting a block of zeros under a given key. The first six digits of the resulting ciphertext is the key check value for that key.

NOTE: *Some hardware security modules only return the first four digits.*

The key check value does not need to be protected since it cannot be used to backtrack to the cleartext key. Because the encryption of zeros under the same key always yields the same results, the key check value can be used to verify that two copies of a key are in fact identical.

Figure 7–3 provides a sample of the procedure required to generate a key check value.

Figure 7–3: Sample Key Check Value



7.6 Dynamic Key Exchange (DKE) Service

The Dynamic Key Exchange Service (DKE) is an optional Visa service that enables members to periodically change the working keys used to protect cardholder PINs. These keys can be changed dynamically through the exchange of online messages.

NOTE: *This service is only available for members using the Single Message System (SMS). Members implementing should also reference the* October 2000 VisaNet Business Enhancements Member Implementation Guide.

7.6.1 Overview

The Dynamic Key Exchange Service offers members two alternatives for key conveyance, both of which protect PINs from disclosure during transmission.

- The member sends an administrative request to Visa for a new acquirer or a new issuer working key. After receiving the request, Visa generates the appropriate working key and sends it online to the member.
- The member authorizes Visa to automatically generate new acquirer and new issuer working keys on a daily basis. The member may specify the time of day when Visa should generate and send new keys before sending an authorization request to the issuer.

Keys are exchanged using 0800 and 0810 network management messages.

7.6.2 Member Participation Requirements

To participate in the Dynamic Key Exchange Service, an acquirer or issuer must notify Visa. Certification for this service will be required.

Participating members must complete the Key Management and ZCMK Request forms using the method described in the section, “Zone Control Master Key (ZCMK)”. Visa will generate the Zone Control Master Key and component working keys and send them to the member in a secure mailer within 14 days of receipt of the forms. This initial paperwork must be completed prior to establishing the actual Dynamic Key Exchange Service.

7.6.3 Service Description

When a member begins participating in Dynamic Key Exchange, all working keys will be protected during online transmission by encrypting new keys with a Key Exchange Key (KEK). The KEK is derived from variant-1 of the ZCMK. Variant-1 is obtained by exclusive-ORing the ZCMK with a value of 0800000000000000.

A 4-digit check value will be included in the 0800 online message to verify receipt of the new working key. Members should compare the first four check digits returned from their security module with the check value in the message. If the check digits do not match or if a security module error is encountered while attempting to translate the new key for storage, the member should return a response code of 06. This will indicate that the new working key has not been received properly.

7.6.4 Acquirer and Issuer Working Keys

In the Dynamic Key Exchange environment, two acquirer and two issuer working keys are available. The Zone Key Index in Field 53—Security Related Control Information of the 0800 message indicates the key used to encrypt the PIN. For a participant in Dynamic Key Exchange, the two keys will be used interchangeably as active and alternate keys. In Dynamic Key Exchange messages, the Zone Key Index will also be used to indicate the key being changed. To ensure that messages can be completed during a key exchange session, the alternate key (the key that is not in use) is changed while the active key is used. For more information on this field, refer to the section "Security-Related Control Information".

NOTE: *Members using Triple DES should also see the* October 2000 VisaNet Business Enchancements Member Implementation Guide.

7.6.5 Multiple Stations

If multiple stations interface with VisaNet, one station may be designated to receive all acquirer key management messages and another station named to receive all issuer messages. If no stations are designated, VisaNet will select an appropriate acquirer or issuer station. Acquirers or issuers do not have to be signed on to a station in order to receive key management messages.

7.6.6 Time-Out Values

Visa will set a 10-second time-out value for all messages containing a new working key. If the member does not respond within 10 seconds or if the member responds indicating an improper receipt of the new key, Visa will re-send the key delivery message. If the second attempt to deliver the new key fails, the key change will be canceled.

If a member encounters encryption or decryption errors from their security module, they should respond to Visa with Response Code 81—Cryptographic Error Found in PIN. Response code 81 is used when a security module finds a cryptographic error during PIN decryption. Visa will generate and send a new working key to the member.

7.6.7 Field Usage for 0800 and 0810 Online Messages

The following fields will be used in the Dynamic Key Exchange Service:

7.6.7.1 Forwarding Institution Identification Code—Field 33

Field 33 contains the 6-digit BIN to which the new working key is applied. This field is present in all Dynamic Key Exchange messages.

7.6.7.2 Response Code—Field 39

Field 39 is used in 0810 response messages to acknowledge receipt of the request message and to indicate the ability of Visa (or the member) to comply with the request. The following response codes are used:

Response Code 00: Request Acknowledged (will comply)

Visa returns Response Code 00 when it accepts the member's request for a key change. The member must use this response code to indicate that the acquirer or issuer working key has been accepted and is ready for use.

Response Code 06: Request Acknowledged (unable to comply)

Visa returns Response Code 06 when it cannot accept a member's request for a key change. This condition occurs if the identifying institution is not set up as a Visa participant in the Dynamic Key Exchange Service, or if a key change is already in progress when the request is received. This condition also occurs if a key change request has the wrong Zone Key Index in field 53. For example, if an acquirer sends a request with a key index of 01 and 01 is the current active key, V.I.P. will respond with a Code 06. The member must use this code when it cannot accept the new key.

Response Code 81: Cryptographic Error Found In PIN

The member returns Code 81 to Visa when a security module finds a cryptographic error during PIN decryption.

7.6.7.3 Additional Data Private—Field 48

Field 48 is used for working key check digits and is present in 0800 requests with Network Management codes 162 and 163 (field 70).

The format of field 48 is described as follows:

- Field Length: 1 byte binary
- Field Identifier: & (ampersand) character (EBCDIC)
- Check Digits: 4 alphanumeric characters (EBCDIC)

The check digits are the first four hexadecimal digits of output resulting from encrypting zeros with the newly issued key in Field 96—Message Security Code.

7.6.7.4 Security-Related Control Information—Field 53

Field 53 is used to indicate which of the two possible working keys is to be changed:

- Value 01: Working Key 1 is to be changed
- Value 02: Working Key 2 is to be changed. Field 53 is required in all incoming 0800 messages involving key exchange.

The member must indicate which key is to be changed in the Request for Key messages. V.I.P. will also use this field in outgoing 0800 messages to indicate which key is to be updated when initiating messages to Deliver New Keys.

7.6.7.5 Network ID Code—Field 63.1

Field 63.1 is used for the Network Identification Code of the BIN to which the new working key applies. The field is present in all dynamic key exchange messages. The format of the field is as follows:

- Field Length: 1 byte binary, value = 06
- Internal Field Map: 3 bytes, value = 800000
- Network ID Code: 2 bytes
- Values:
  - Visa: 0002
  - Interlink: 0003
  - Plus: 0004

NOTE: *If members are using the same IWKs and AWKs for multiple services, they may choose to use one network ID for key exchange. The keys will apply to all applicable services.*

7.6.7.6 Network Management Information Code— Field 70

Field 70 is present in all messages and contains one of the following values:

- Request for generation of new AWK (acquirer to Visa): 160
- Request for generation of new IWK (issuer to Visa): 161
- Deliver new AWK (Visa to acquirer): 162
- Deliver new IWK (Visa to issuer): 163

7.6.7.7 Message Security Code—Field 96

Field 96 is used for the new working key and is present in all 0800 messages with Network Management codes 162 and 163.

NOTE: *Field 105 is used for Triple DES. SMS acquirers using Dynamic Key Exchange must modify their systems to accept SMS 0800 messages with Field 105-Double-Length DES Key (Triple DES) instead of Field 96—Message Security Code. DKE requires certification.*

7.6.8 Message Matrix

Figure 7–4 depicts the message field matrix for Network Management messages for the Dynamic Key Exchange Service.

Figure 7–4: Message Matrix

Field		VisaNet	
		0800	0810
Number	Field Name	Sender	Receiver
1	Secondary Field Map	M	M
7	Transmission Date and Time	M	M
11	Systems Trace Audit Number	M	M
33	Forwarding Institution ID	M	M
39	Response Code		M
48P	Additional Data - Private	C	
53	Security Related Cont. Inf.	M	
63.1	Network ID Code	M	M
70	Network Management Info. Code	M	M
96	Message Security Code	C	

M = Mandatory, field/value must be present in the message.
C = Conditional, field/value is present in the message under certain conditions as outlined in Volume 2 of the *V.I.P. Technical Reference manual.*

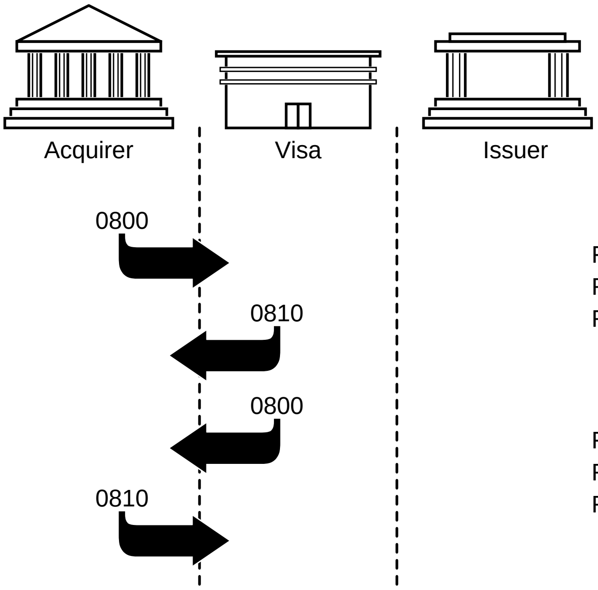
7.6.9 Message Flows

This section contains message flow diagrams for acquirers or issuers requesting the generation of new keys and automatic keys. The following sections describe the normal cases and various exception scenarios.

7.6.9.1 Acquirer Requests New Key Generation

In this scenario, the acquirer asks Visa to change the AWK. Figure 7–5 depicts the message flows for this process.

Figure 7–5: Acquirer Requests New Key Generation



Flow Direction: Acquirer ➞ Visa
Request Message: 0800 (NMI=160, Generate New Key)
Response Message: 0810 (NMI=160)

Flow Direction: Visa ➞ Acquirer
Request Message: 0800 (NMI=162, Deliver New Key)
Response Message: 0810 (NMI=162)

The steps for this process are as follows:

1. The acquirer sends an 0800 message to Visa. The Zone Key Index in field 53 indicates that the alternate key (the key currently not in use) is to be changed.

2. Visa responds with an 0810 message indicating that the request was accepted. If an incorrect Zone Key Index was in the 0800 message, the 0810 response will contain response code 06 (Request Acknowledged, Unable to Comply).

3. Visa generates a new AWK, encrypts it under the Key Exchange Key that was established for the member (Variant-1 of the ZCMK), and sends an 0800 message to the member with the new key and corresponding check digits. The Zone Key Index will match the index received in the Request for Key Change message, indicating that the alternate key is to be updated by the acquirer.

4. The acquirer validates the key by encrypting zeros and comparing the check value. If the key passes all validation tests and does not contain any security module errors and the check digits returned from the acquirer's security module match those in the 0800 message, the acquirer sends an 0810 message with response code 00, which indicates acceptance.

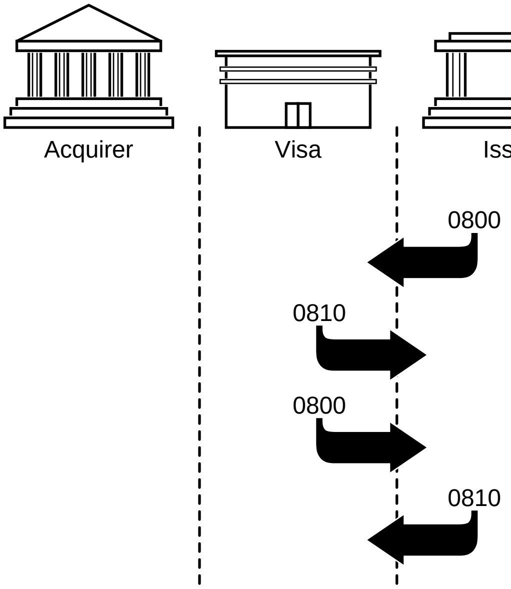
   Otherwise, response code 06, which indicates an error, is sent.

5. The acquirer may begin using the new key after the 0810 response is sent to Visa. Visa must be informed of which of the two AWKs has been used to encrypt the PIN in each key exchange message. The acquirer indicates which key by using the appropriate Zone Key Index in Field 53 of the acceptance message.

7.6.9.2 Issuer Requests New Key Generation

In this scenario, the issuer asks Visa to change the IWK. Figure 7–6 depicts the message flows for this process.

Figure 7–6: Issuer Requests New Key Generation



Flow Direction: Issuer → Visa
Request Message: 0800 (NMI=161, Generate New Key)
Response Message: 0810 (NMI=161)

Flow Direction: Visa → Issuer
Request Message: 0800 (NMI=163, Deliver New Key)
Response Message: 0810 (NMI=163)

The steps for this process are as follows:

1. The issuer sends an 0800 message to Visa. The Zone Key Index in field 53 indicates that the alternate key (the key currently not in use) is to be changed.

2. Visa responds with an 0810 message indicating that the request was accepted. If an incorrect Zone Key Index was in the 0800 message, the 0810 response will contain response code 06.

3. Visa immediately generates a new IWK, encrypts it under the Key Exchange Key that was established for the member (Variant-1 of the ZCMK), and sends an 0800 message to the member with the new key and corresponding check digits. The Zone Key Index will be the same as that received in the request for key change messages, thereby indicating that the alternate key is to be updated by the issuer.

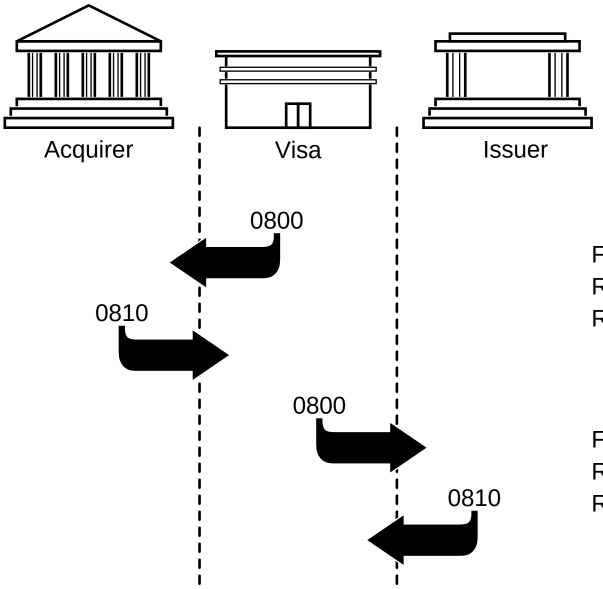
4. The issuer validates the key and check digits. If the key passes all validation tests and does not contain any security module errors and the check digits returned from the issuer's security module match those in the 0800 message, the issuer sends an 0810 message with a response code of 00, which indicates acceptance. Otherwise, Response Code 06, which indicates an error, is sent.

5. Visa will begin using the new key after the 0810 response (with Response Code 00) is received from the issuer. The issuer is told which of the two issuer keys was used to encrypt the PIN in each message. This is accomplished using the appropriate Zone Key Index in field 53 of the message.

7.6.9.3 Automatic New Key Generation

In this scenario, the acquirer or issuer has indicated that Visa should periodically issue new acquirer working keys, issuer working keys, or both. Figure 7–7 depicts the message flows for this process.

Figure 7–7: Automatic New Key Generation



Flow Direction: Visa → Acquirer
Request Message: 0800 (NMI=162, Generate New Key)
Response Message: 0810 (NMI=162)

Flow Direction: Visa → Issuer
Request Message: 0800 (NMI=163, Deliver New Key)
Response Message: 0810 (NMI=163)

The steps for the generation and delivery of the keys are similar to those described in previous flows, with the exception that transmission will occur without the member sending an 0800 request. In these cases, Visa will always set Zone Key Index in field 53 to the alternate (not in use) key.

7.6.9.4 Exception Conditions

The following exception conditions may occur during the Dynamic Key Exchange process. Each condition's description includes the action that Visa will take and the recommended action (if any) that the member should take.

- Undeliverable response

  If Visa cannot deliver an 0810 response to a member's request for key generation, the 0810 message will be discarded. However, the 0800 key delivery message will still be sent to the member. Therefore, the member should be able to process the 0800 message even if the 0810 response does not arrive.

- Undeliverable request

  If Visa cannot deliver a new key, it will discard the 0800 message and process it as if a timeout occurred.

- Timeout

  If Visa does not receive a response to an 0800 key delivery message within 10 seconds, V.I.P. will re-send the request. If no response is received to the second request, Visa will cancel the key change.

- PIN block errors

  If Visa encounters PIN block errors while attempting to de-encrypt the acquirer's PIN block, Visa will return a Response Code of 81 to the authorization or financial transaction. Visa will then initiate an automatic key change for the AWK.

  During normal transaction processing, if the issuer encounters PIN block errors while attempting to verify the PIN, the issuer must return a response code of 81 to Visa. Visa will then initiate an automatic key change for the IWK.

- Visa not accepting key change messages

  If an acquirer or issuer initiates a request for a new working key and VisaNet is temporarily unable to accept key management messages, Visa will return a 0810 response with Response Code of 06. The member may reinitiate the key change request at a later time.

7.6.10 Implementation Considerations

Both acquirers and issuers should evaluate possible alternative processes if problems are encountered during the implementation. It is recommended that a procedure be established to allow a return to manual key procedures. Visa offers the following two procedures:

- Offline

  When a key problem is discovered, Visa will contact the member or the member will contact Visa and the further generation of working keys is temporarily halted. When the Offline procedure is invoked, Visa will start using the static key in messages sent to the member. The operator at the member site must be familiar with the procedure for transferring their static keys to their dynamic key areas; the method for doing this will vary by member. Once this static key is in place, Visa will coordinate with the member to return to dynamic keys.

- Fallback

  When the Fallback option is used, Visa will send the member an 0800 key exchange message in which the key in field 96 is equal to zeros. When field 96 is filled with zeros, the members should switch to their static keys and send a 0810 response with Response Code Zero (Field 39). If the member does not respond with an approval, V.I.P. will not use the static key. This Fallback procedure is similar to the normal key exchange process, except that field 96 contains zeros.

  While members may choose Offline or Fallback, the recommended option is Offline. With this option, members are not dependent upon the exchange of online messages to confirm delivery or receipt of the static key.

7.7 Exchange of Double-Length Keys

Double-length keys may be exchanged either electronically or as hard copy cleartext components.

Electronic key conveyance is described in the section, “Dynamic Key Exchange Service.”

Hard copy key conveyance will take place following completion and receipt of the appropriate Key Management forms. Three 32-character[1] components will be sent under separate cover and by different routes to the Key Custodians designated in the Key Conveyance forms. The Key Custodians will then enter their individual components as described in the section, “Zone Control Master Key (ZCMK)”.

The following section describes how to process a set of double-length key exchange, key clear components, and a double-length key.

7.7.1 Assumptions

The procedures describe below include the following assumptions about the device or system being used.

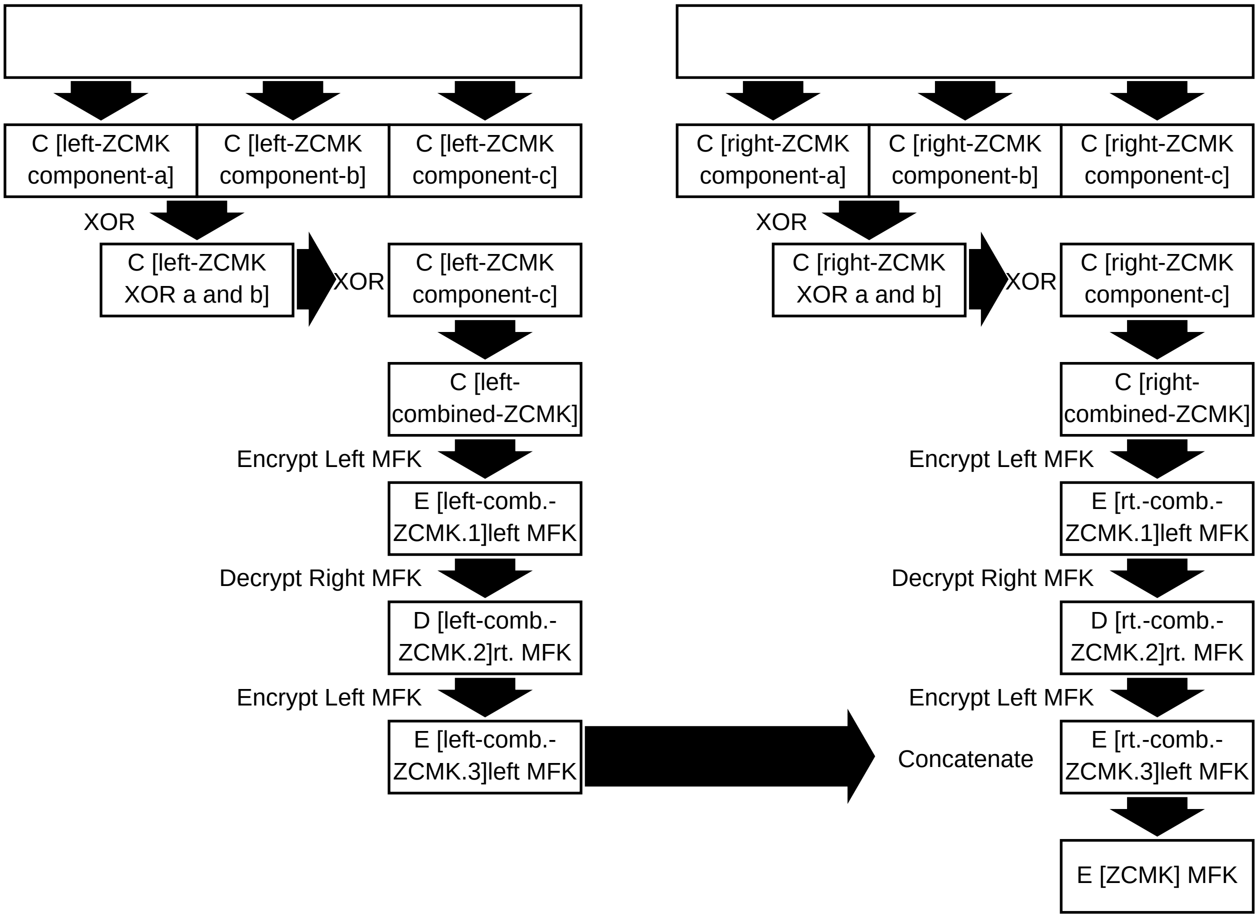
- The device or system uses a 32-digit double-length Master File Key (MFK).
- The device or system can perform an encrypt-decrypt-encrypt operation.

[1] Single-length key conveyance consists of two or three, 16-character components.

7.7.1.1 Double-Length Key Exchange Keys

The following procedure describes the generation of double-length ZCMKs, which are delivered as three cleartext 32-digit components. Figure 7–8 depicts this process which is detailed later.

Figure 7–8: Generation of Double-Length Key Exchange Keys


C [left-ZCMK component-a]
C [left-ZCMK component-b]
C [left-ZCMK component-c]
XOR
C [left-ZCMK XOR a and b]
XOR
C [left-ZCMK component-c]
C [left-combined-ZCMK]
Encrypt Left MFK
E [left-comb.-ZCMK.1]left MFK
Decrypt Right MFK
D [left-comb.-ZCMK.2]rt. MFK
Encrypt Left MFK
E [left-comb.-ZCMK.3]left MFK
C [right-ZCMK component-a]
C [right-ZCMK component-b]
C [right-ZCMK component-c]
XOR
C [right-ZCMK XOR a and b]
XOR
C [right-ZCMK component-c]
C [right-combined-ZCMK]
Encrypt Left MFK
E [rt.-comb.-ZCMK.1]left MFK
Decrypt Right MFK
D [rt.-comb.-ZCMK.2]rt. MFK
Encrypt Left MFK
E [rt.-comb.-ZCMK.3]left MFK
Concatenate
E [ZCMK] MFK

1. Divide each 32-hex digit clear component into a 16-hex digit left half and a 16-hex digit right half. This should result in a total of six, 16-digit clear components that are labeled as follows:
   - C [left-ZCMK-component-a]
   - C [left-ZCMK-component-b]
   - C [left-ZCMK-component-c]
   - C [right-ZCMK-component-a]
   - C [right-ZCMK-component-b]
   - C [right-ZCMK-component-c]
2. XOR the left-ZCMK components as follows:
   a. XOR C [left-ZCMK-component-a] with
   b. C [left-ZCMK-component-b]
   c. XOR the result from step a with C [left-ZCMK-component-c]
   d. The result of step b is a clear-combined left half of the ZCMK labeled: C [left-combined-ZCMK]
3. XOR the right-ZCMK components as follows:
   a. XOR C [right-ZCMK-component-a] with
   b. C [right-ZCMK-component-b]
   c. XOR the result from step a with C [right-ZCMK-component-c]
   d. The result of step b is a clear-combined right half of the ZCMK labeled C [right-combined-ZCMK]
4. Encrypt-decrypt-encrypt the left-combined-ZCMK components as follows:
   a. ƒ Encrypt C [left-combined-ZCMK] left MFK giving a result labeled: E [left-combined-ZCMK.1] left MFK
   b. ƒ Decrypt E [left-combined-ZCMK.1] right MFK giving a result labeled: D [left-combined-ZCMK.2] right MFK
   c. ƒ Encrypt D [left-combined-ZCMK.2] left MFK giving a result labeled: E [left-combined-ZCMK.3] left MFK
5. Encrypt-decrypt-encrypt the right-combined-ZCMK components as follows:
   a. ƒ Encrypt C [right-combined-ZCMK] left MFK giving a result labeled: E [right-combined-ZCMK.1] left MFK
   b. ƒ Decrypt E [right-combined-ZCMK.1] right MFK giving a result labeled: D [right-combined-ZCMK.2] right MFK

c. ƒ Encrypt D [right-combined-ZCMK.2] left MFK giving a result labeled: E [right-combined-ZCMK.3] left MFK

6. Concatenate E [left-combined-ZCMK.3] left MFK and E [right-combined-ZCMK.3] left MFK giving a result labeled: E [ZCMK] MFK

7.7.1.2 Key Check Value

A key check value can be calculated by using the clear right-combined-ZCMK and the left-combined-ZCMK to perform an encrypt-decrypt-encrypt operation against 16-hex zeros. The procedure is as follows:

1. ƒ Encrypt C [16-hex-zeros] left-combined-ZCMK giving a result labeled: E [16-hex-zeros] left-combined-ZCMK
2. ƒ Decrypt E [16-hex-zeros] right-combined-ZCMK giving a result labeled: D [16-hex-zeros] right-combined-ZCMK
3. ƒ Encrypt D [16-hex-zeros] left-combined-ZCMK giving a result labeled: ZCMK-key-check-value.

7.7.2 Double-Length Master Derivation Key Processing

7.7.2.1 Assumptions

The procedures described below include the following assumptions:

- A double-length working key is being processed, not a pair of single-length keys.
- A double-length KEK is being used to import or export the working key.

7.7.2.2 Double-Length Working Key

The following procedure describes the generation of double-length working keys as 32-hex digit keys that are delivered encrypted under a double-length KEK:

1. Divide the 32-hex digit encrypted working key into a 16-hex digit left half and a 16-hex digit right half and label these as:
   - E [left-working-key] ZCMK
   - E [right-working-key] ZCMK
2. Within a Host Security Module, the encrypted ZCMK is decrypted and divided into a 16-hex digit left half and a 16-hex digit right half and labeled as:
   - C [left ZCMK]
   - C [right ZCMK]

3. To decrypt the left half of the working key, perform the following:

   a. ƒ Decrypt E [left-working-key] left ZCMK giving a result labeled:
   C [left-working-key.1] left ZCMK

   b. ƒ Encrypt C [left-working-key.l] right ZCMK giving a result labeled:
   E [left-working-key.2] right ZCMK

   c. ƒ Decrypt E [left-working-key.2] left ZCMK giving a result labeled:
   C [left-working-key.3] left ZCMK

4. To decrypt the right half of the working key perform the following:

   a. ƒ Decrypt E [right-working-key] left ZCMK giving a result labeled:
   C [right-working-key.1] left ZCMK

   b. ƒ Encrypt C [right-working-key.1] right ZCMK giving a result labeled:
   E [right-working-key.2] right ZCMK

   c. ƒ Decrypt E [right-working-key.2] left ZCMK giving a result labeled:
   C [right-working-key.3] left ZCMK

5. To translate the now clear working key left half into encryption under a Host Security Module’s MFK, perform the following:

   a. ƒ Encrypt C [left-working-key] left MFK giving a result labeled:
   E [left-working-key.1] left MFK

   b. ƒ Decrypt E [left-working-key.1] right MFK giving a result labeled:
   E [left-working-key.2] right MFK

   c. ƒ Encrypt E [left-working-key.2] left MFK giving a result labeled:
   E [left-working-key.3] left MFK

6. To translate the now clear working key right half into encryption under a Host Security Module's MFK, perform the following:

   a. ƒ Encrypt C [right-working-key] left MFK giving a result labeled:
   E [right -working-key.1] left MFK

   b. ƒ Decrypt E [right-working-key.1] right MFK giving a result labeled:
   E [right-working-key.2] right MFK

   c. ƒ Encrypt E [right-working-key.2] left MFK giving a result labeled:
   E [right-working-key.3] left MFK

7. Concatenate E [left-working-key.3] left MFK and E [right-working-key.3] left MFK giving a result labeled: E [working-key] MFK

8. Calculate a key check value as described in “Double-Length Key Exchange Keys”. The clear left and right halves of the working key must be substituted into the procedure.

Track 1 Data A

This appendix describes Visa standards for the contents of Track 1 of the magnetic stripe and the magnetic stripe image on the integrated chip. Visa requirements conform to the International Organisation for Standardisation (ISO) standard 7811/2, *Identification cards—Recording technique—Part 2: Magnetic Stripe* and ISO standard 7813, *Identification Cards—Financial Transaction Cards*.

A.1 Track 1 Content Requirements

Requirements for the contents of the magnetic stripe conform to ISO 7813.

Specifications for the physical placement of the magnetic stripe on a card are in *Visa International Operating Regulations, Volume III—Card and Marks Specifications*.

A.2 Record Format

Table A–1 displays the Track 1 record format for a magnetic stripe. With the exception of the following list, all fields are required in Track 1 of the magnetic stripe track:

- The PIN Verification Data field is optional for all cards with the exception of Visa Gold/Premier cards.
- The Discretionary Data field is optional.
- The Authorization Control Indicator (ACI) in the Visa-Reserved field is optional.
- A Card Verification Value (CVV) is required in the Visa-Reserved field on all Visa, Visa Electron, and Plus cards.

Figure A–1 lists the Track 1 field names and their length. The maximum length of Track 1 is 79 characters. Refer to "Data Element Descriptions" for more information.

Figure A–1: Track 1 Record Format

Field Number	Length	Field Name		
1	1	Start Sentinel		
2	1	Format Code		
3	13 or 16	Primary Account Number (PAN)		
4	1	Separator		
5	2 to 26	Cardholder Name		
6	1	Separator		
7	4	Card Expiration Date		
8	3	Service Code		
9	0 or 5	PIN Verification		
		Position	Length	Content
		1	1	PIN Verification Key Index PVKI)
		2 to 5	4	PIN Verification Value (PVV)
10	Varies[1]	Discretionary Data		
11	11[2]	Visa Reserved		
		Position	Length	Content
		1 to 2	2	Zero fill
		3 to 5	3	Card Verification Value (CVV)
		6 to 7	2	Zero fill
		8	1	Authorization Control Indicator (ACI)
		9 to 11	3	Zero fill
		All 11 positions are required		
12	1	End Sentinel		
13	1	Longitudinal Redundancy Check (LRC)		

[1] The length of this field depends on the lengths of fields 3, 5 and 9.

[2] The length is always the last 11 positions of Track 1, excluding the End Sentinel and Longitudinal Redundancy Check.

A.3 Character Set

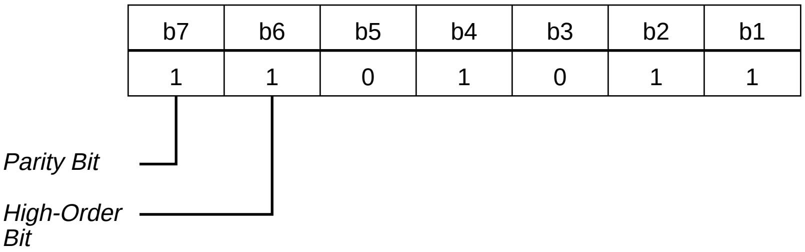
The bit-sequence pattern for the letter K is illustrated in Figure A–2.

Table A–1 describes the Track 1 character set. This table corresponds to the comparable table in Section 10.1.3 of ISO standard 7811/2.

Data formats to be provided to an encoding machine are specified by the hardware manufacturer. The encoding device must use odd parity to encode data characters. Clocking bits for synchronization are not considered as data.

Additionally, an even-parity Longitudinal Redundancy Check character must be the last character in a track record.

Figure A–2: Letter K Bit-sequence Pattern



b7	b6	b5	b4	b3	b2	b1
1	1	0	1	0	1	1

NOTE: *The parity bit is automatically generated and encoded by the encoding machine.*

The encoding equipment must encode the magnetic stripe data of Track 1 in accordance with the bit-sequence patterns specified in Figure A–2.

NOTE: *bn = bit position number “n.”*

Table A–1: Track 1 Character Set (1 of 4)

Char.	Hex	Binary						
		P	2^5	2^4	2^3	2^2	2^1	2^0
space	20	1	0	0	0	0	0	0
!	21	0	0	0	0	0	0	1
“	22	0	0	0	0	0	1	0
#	23	1	0	0	0	0	1	1
$	24	0	0	0	0	1	0	0
%	25	1	0	0	0	1	0	1
&	26	1	0	0	0	1	1	0
‘	27	0	0	0	0	1	1	1
(	28	0	0	0	1	0	0	0
)	29	1	0	0	1	0	0	1
*****	2A	1	0	0	1	0	1	0
+	2B	0	0	0	1	0	1	1
,	2C	1	0	0	1	1	0	0
-	2D	0	0	0	1	1	0	1
.	2E	0	0	0	1	1	1	0
/	2F	1	0	0	1	1	1	1
0	30	0	0	1	0	0	0	0
1	31	1	0	1	0	0	0	1

Table A–1: Track 1 Character Set (2 of 4)

Char.	Hex	Binary						
		P	2^5	2^4	2^3	2^2	2^1	2^0
2	32	1	0	1	0	0	1	0
3	33	0	0	1	0	0	1	1
4	34	1	0	1	0	1	0	0
5	35	0	0	1	0	1	0	1
6	36	0	0	1	0	1	1	0
7	37	1	0	1	0	1	1	1
8	38	1	0	1	1	0	0	0
9	39	0	0	1	1	0	0	1
:	3A	0	0	1	1	0	1	0
;	3B	1	0	1	1	0	1	1
<	3C	0	0	1	1	1	0	0
=	3D	1	0	1	1	1	0	1
>	3E	1	0	1	1	1	1	0
?	3F	0	0	1	1	1	1	1
@	40	0	1	0	0	0	0	0
A	41	1	1	0	0	0	0	1
B	42	1	1	0	0	0	1	0
C	43	0	1	0	0	0	1	1
D	44	1	1	0	0	1	0	0

Table A–1: Track 1 Character Set (3 of 4)

Char.	Hex	Binary						
		P	2^5	2^4	2^3	2^2	2^1	2^0
E	45	0	1	0	0	1	0	1
F	46	0	1	0	0	1	1	0
G	47	1	1	0	0	1	1	1
H	48	1	1	0	1	0	0	0
I	49	0	1	0	1	0	0	1
J	4A	0	1	0	1	0	1	0
K	4B	1	1	0	1	0	1	1
L	4C	0	1	0	1	1	0	0
M	4D	1	1	0	1	1	0	1
N	4E	1	1	0	1	1	1	0
O	4F	0	1	0	1	1	1	1
P	50	1	1	1	0	0	0	0
Q	51	0	1	1	0	0	0	1
R	52	0	1	1	0	0	1	0
S	53	1	1	1	0	0	1	1
T	54	0	1	1	0	1	0	0
U	55	1	1	1	0	1	0	1
V	56	1	1	1	0	1	1	0
W	57	0	1	1	0	1	1	1

Table A–1: Track 1 Character Set (4 of 4)

Char.	Hex	Binary						
		P	2^5	2^4	2^3	2^2	2^1	2^0
X	58	0	1	1	1	0	0	0
Y	59	1	1	1	1	0	0	1
Z	5A	1	1	1	1	0	1	0
[	5B	0	1	1	1	0	1	1
\	5C	0	1	1	1	1	0	0
]	5D	0	1	1	1	1	0	1
^	5E	0	1	1	1	1	1	0
_	5F	1	1	1	1	1	1	1

NOTE: *This coded character set is identical to the coded character set in ISO/IEC 7811-4 and is derived from ASCII.*

A.4 Encoding Examples

This section contains four examples of Track 1 encoding.

NOTE: *The examples provide a sample format only and should not be followed literally when encoding Track 1 of the magnetic stripe.*

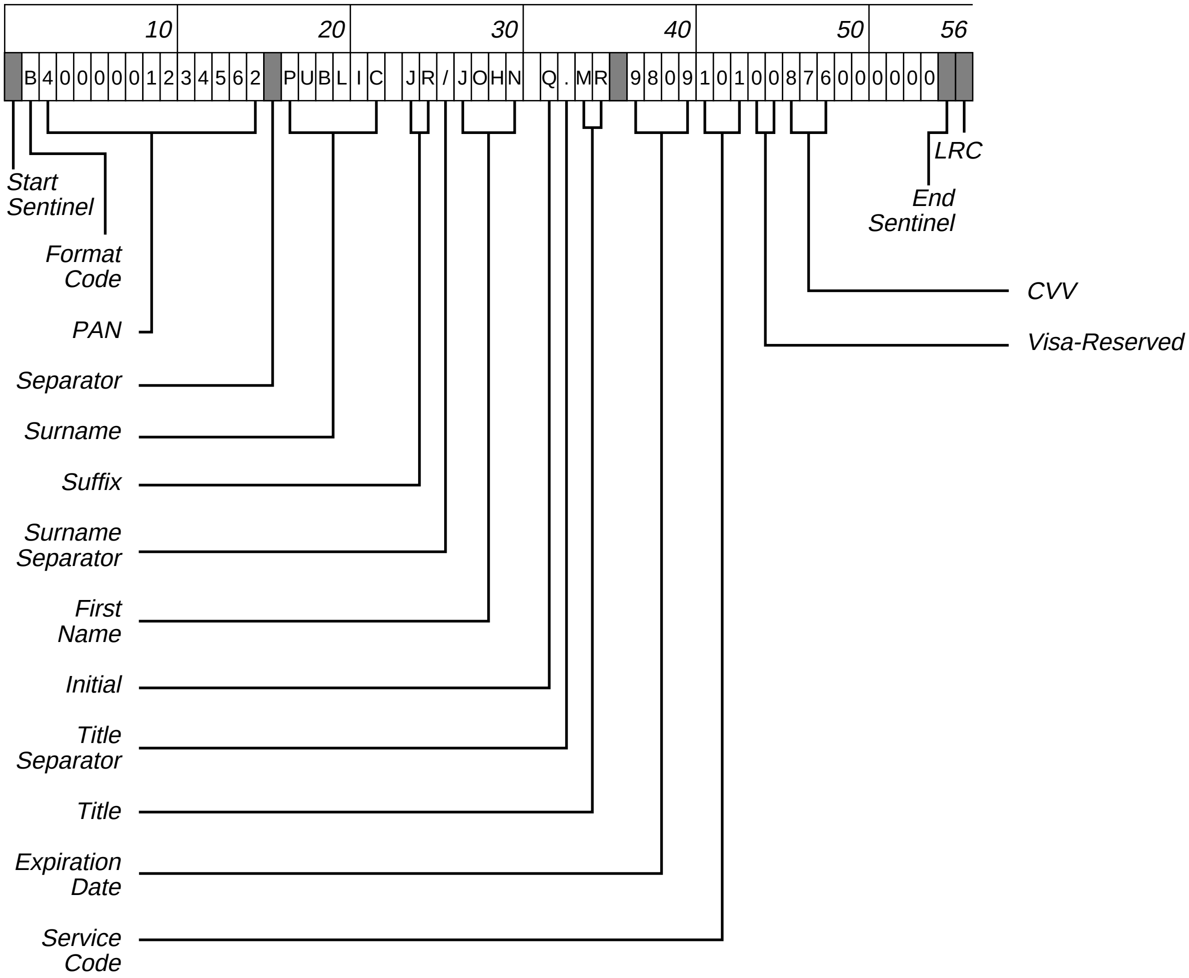
- Figure A–3 illustrates encoding with the required fields. The optional PIN Verification Data and Discretionary Data fields are not used in this example. The Visa-Reserved field shows the position of the CVV.
- Figure A–4 illustrates encoding with the PIN Verification Data field. The Visa-Reserved field shows the position of the CVV.
- Figure A–5 illustrates encoding with the Discretionary Data field. The Visa-Reserved field shows the position of the CVV.
- Figure A–6 illustrates encoding with both optional fields. The Visa-Reserved field shows the position of the CVV.

A.4.1 Example 1: Encoding Required Fields

Information to be encoded:

- PAN: 4000 00l2 3456 2 (13 digits)
- Cardholder Name: MR JOHN Q PUBLIC JR
- Expiration Date: 09/98
- Service Code: 101
- PIN Verification Data: none
- Discretionary Data: none
- Visa-Reserved: 11 characters with 876 for the CVV and the remaining positions are zero-filled

Figure A–3: Encoding Required Fields

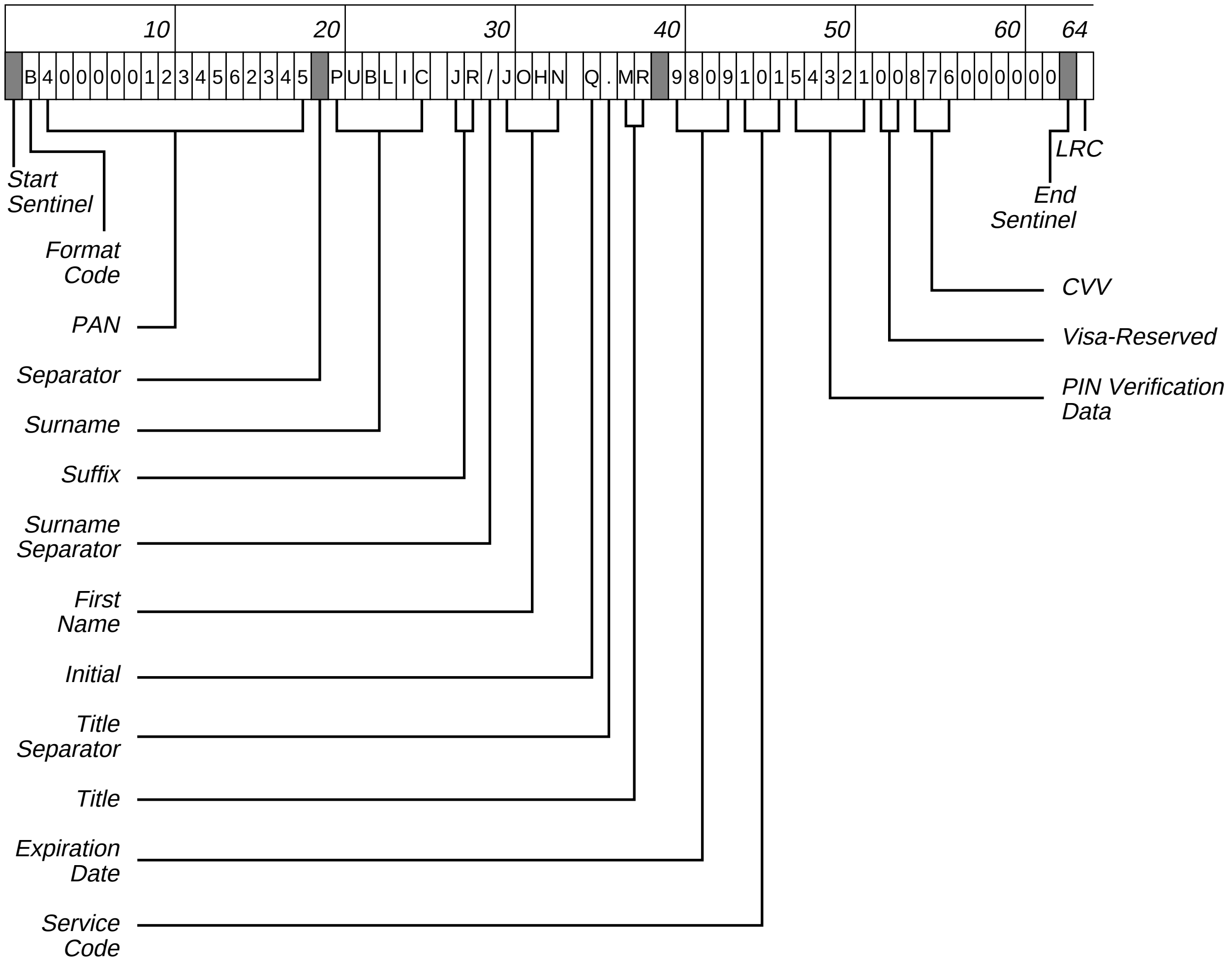


A.4.2 Example 2: Encoding With PIN Verification Data Field

Information to be encoded:

- PAN: 4000 0012 3456 2345 (16 digits)
- Cardholder Name: MR JOHN Q PUBLIC JR
- Expiration Date: 09/98 Service Code: 101
- PIN Verification Data: 5 (PVKI) and 4321 (PVV)
- Discretionary Data: none
- Visa-Reserved: 11 characters with 876 for the CVV and the remaining positions are zero-filled

Figure A–4: Encoding With PIN Verification Data Field

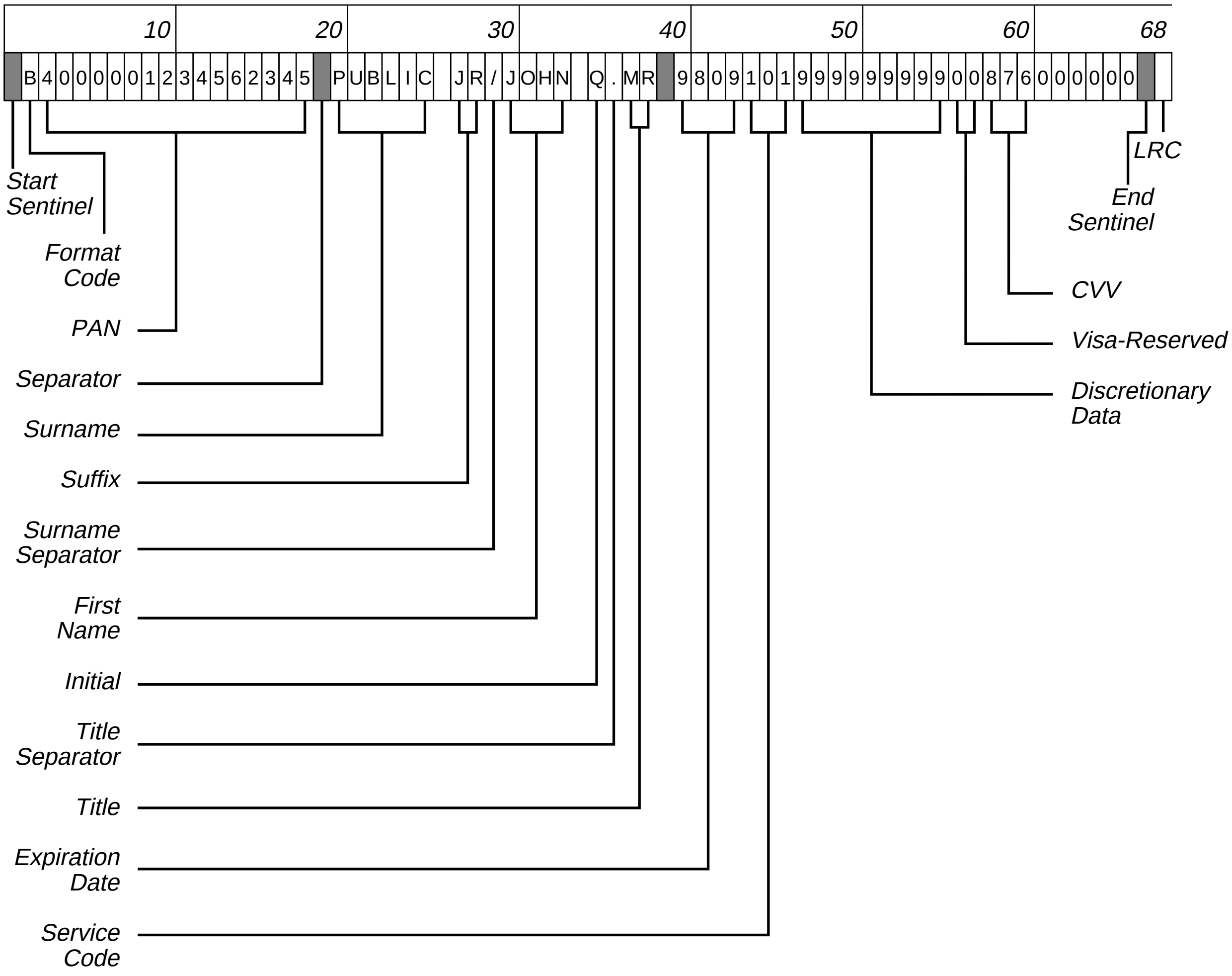


A.4.3 Example 3: Encoding With Discretionary Data Field

Information to be encoded:

- PAN: 4000 0012 3456 2345 (16 digits)
- Cardholder Name: MR JOHN Q PUBLIC JR
- Expiration Date: 09/98
- Service Code: 101
- PIN Verification Data: none
- Discretionary Data: 999999999
- Visa-Reserved: 11 characters with 876 for the CVV and the remaining positions are zero-filled

Figure A–5: Encoding With Discretionary Data Field

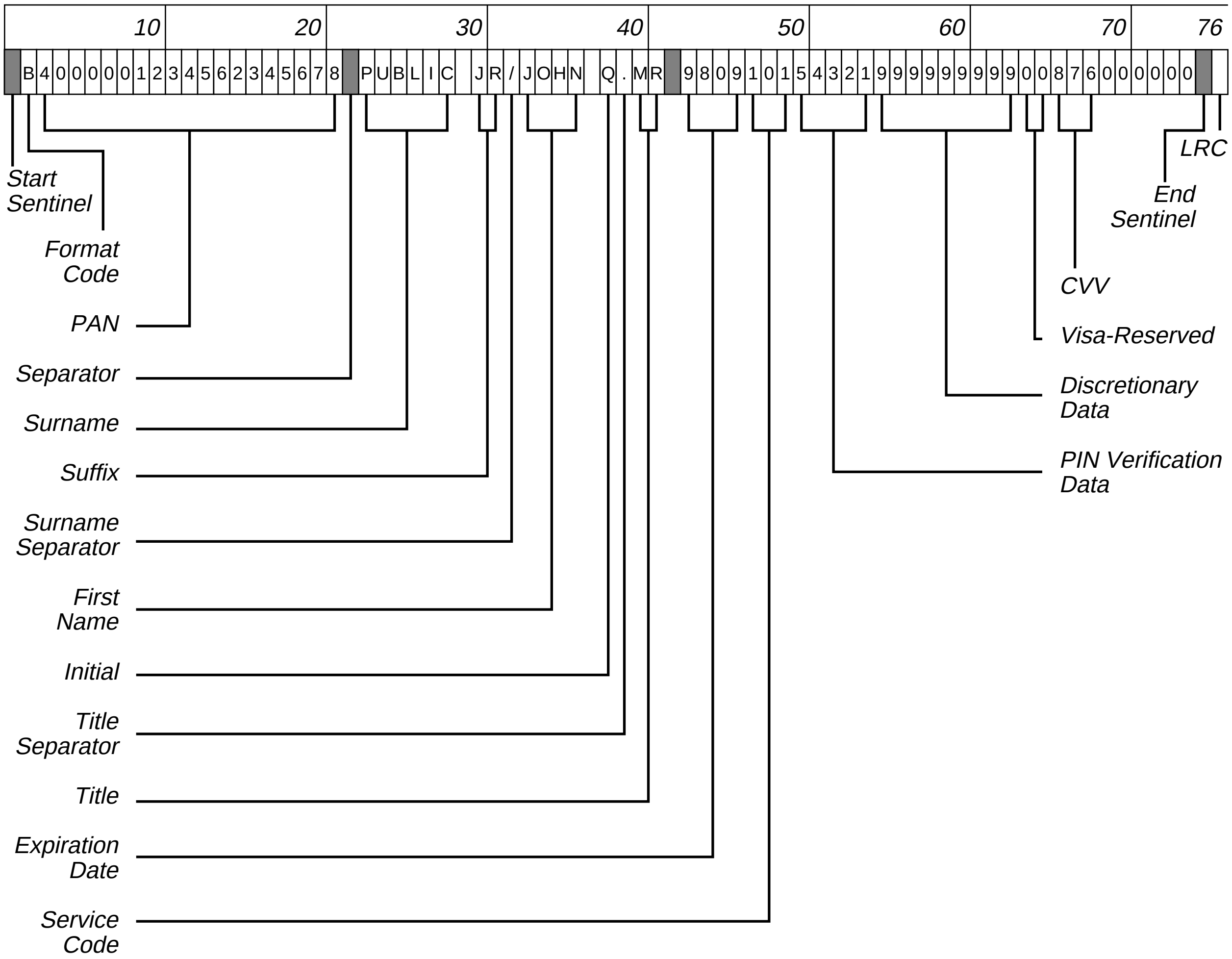


A.4.4 Example 4: Encoding With PIN Verification Data and Discretionary Data Fields

Information to be encoded:

- PAN: 4000 0012 3456 2345 678 (19 digits)
- Embossed Cardholder Name: MR JOHN Q PUBLIC JR
- Embossed Expiration Date: 09/98
- Service Code: 101
- PIN Verification Data: 5 (PVKI) and 4321 (PVV)
- Discretionary Data: 999999999
- Visa-Reserved Field: 11 characters with 876 for the CVV and the remaining positions are zero-filled

Figure A–6: Encoding With PIN Verification and Discretionary Data Fields



A.5 Data Element Descriptions

This section describes the data elements encoded on Track 1 of the magnetic stripe. Table A–2 describes the Start Sentinel.

Table A–2: Field 1—Start Sentinel

Attributes	1 alphanumeric
Description	Indicates the initial data position on the track.
Valid value	%

Table A–3 describes the Format Code data element encoded on Track 1 of the magnetic stripe.

Table A–3: Field 2—Format Code

Attributes	1 alphanumeric
Description	Specifies the format for Track 1 encoding
Valid value	B

Table A–4 describes the PAN data element encoded on Track 1 of the magnetic stripe.

Table A–4: Field 3—Primary Account Number (PAN)

Attributes	16 alphanumeric[1]
Description	A number identifying the customer account
Valid value	0 to 9

[1] While the ISO standard accommodates PANs of up to 19 digits, for human readability and data entry purposes, a minimum of the three blanks must be embossed in the PAN. Therefore, the encoding specification is limited to a 16-digit PAN with no blanks encoded. On a card, the PAN is embossed in a 4-4-4-4 grouping (4XXX XXXX XXXX XXXX).

Table A–5 describes the Separator data element encoded on Track 1 of the magnetic stripe.

Table A–5: Field 4—Separator

Attributes	1 alphanumeric
Description	Indicates the end of a variable-length field such as the PAN field.
Valid value	^ (caret)
Usage	The separator used in fields 4 and 6 of the track record is identically defined.

Table A–6 describes the Cardholder Name data element encoded on Track 1 of the magnetic stripe.

Table A–6: Field 5—Cardholder Name

Attributes	2 to 26 alphanumerics
Description	Cardholder's name
Valid value	Surname: • Hyphen (-) for hyphenated surnames • Suffix (optional) • Surname separator (/) • First name and/or initials • Title separator (.) if a title is to be encoded • Title (optional)
Usage	Two delimiters are used in this field to mark the end of the surname (or surname and suffix) and to mark the presence of a title: The surname separator (/) and title separator (.). The format is the same as that specified in ISO 7813, Identification Cards—Financial Transaction Cards. It is recommended that no spaces be encoded between the last character of the name or title and the beginning of the next field. If Track 1 on a Visa Electron card does not contain a specific cardholder name, the generic name ELECTRON VISA CARDHOLDER must be encoded in this field. For airline ticketing, the customer name is the same as that encoded on the stripe. Therefore, an airline would identify a passenger by the encoded surname, with other names and any title used in the order in which they are encoded, that is, the data following the surname separator (/). The format of the name on Track 1 allows for a minimum field length of two positions. The minimum accommodates cases in which a cardholder has a one-character name. Therefore, the second character must be the surname separator to mark the end of the surname. While the formats of encoded names and embossed names will differ, an issuer should try to keep the content of the encoded and embossed names the same.

A.5.1 Cardholder Name Usage Examples

In Figure A–7, the cardholder's name is embossed as DR THOMAS A HARRIS JR. Note that the title separator (.) follows the first name THOMAS and the initial A.

Figure A–7: Cardholder Name Usage Example 1

H	A	R	R	I	S		J	R	/	T	H	O	M	A	S		A	.	D	R

In Figure A–8, the cardholder's name is embossed with initials, such as MRS J L YOUNG.

Figure A–8: Cardholder Name Usage Example 2

Y	O	U	N	G	/	J		L	.	M	R	S

In Figure A–9, the cardholder's name is embossed without a title, such as PAT B SMITH. No title separator (.) or title is encoded.

Figure A–9: Cardholder Name Usage Example 3

S	M	I	T	H	/	P	A	T		B

Figure A–10, the cardholder's surname is hyphenated, such as L ALSHAMARI.

Figure A–10: Cardholder Name Usage Example 4

A	L	-	S	H	A	M	A	R	I	/	L

In Figure A–11, the generic name ELECTRON VISA CARDHOLDER is encoded as follows.

Figure A–11: Cardholder Name Usage Example 5

E	L	E	C	T	R	O	N		V	I	S	A		C	A	R	D	H	O	L	D	E	R	/

Table A–7 describes the Separator data element encoded on Track 1 of the magnetic stripe.

Table A–7: Field 6—Separator

Attributes	1 alphanumeric
Description	Indicates the end of a variable-length field such as the PAN field.
Valid value	^ (caret)
Usage	The separator used in fields 4 and 6 of the track record is identically defined.

Table A–8 describes the Card Expiration Date data element encoded on Track 1 of the magnetic stripe.

Table A–8: Field 7—Card Expiration Date

Attributes	4 numerics in the format: YYMM
Description	Year and month after which the card can no longer be used.
Valid value	YY must be 00 to 99; MM must be 01 to 12
Usage	The YYMM format follows ISO conventions for machine-processable dates. All cards with a Visa, Visa Electron, or Delta mark must have a finite expiration date that is no more than 20 years from the date of card issue.

Table A–9 describes the Service Code data element encoded on Track 1 of the magnetic stripe.

Table A–9: Field 8—Service Code

Attributes	3 numerics
Description	A sequence of digits that, taken as a whole, defines various services; differentiates cards used in international or national interchange; designates PIN requirements; and identifies card restrictions.
Valid value	The values allowed are made up of three individual digits: 1, 2, and 3. To be valid, each digit must be one of the acceptable values listed in Table A–9. These service code values apply to Visa card products (Visa, Plus, Visa Electron, Interlink, and Delta cards). Not all combinations of individually valid digit values result in a valid service code. Also, while a large number of service codes can be constructed from these values, only specific service codes are authorized for individual Visa card products. Table A–10 and Table A–11 describe the service code values that are currently valid for Visa card products.

Table A–10 describes the Service Code Digit Value data element encoded on Track 1 of the magnetic stripe.

Table A–10: Service Code Digit Value Descriptions (1 of 2)

Digit	Value	Description
1	0	Invalid for Visa card products
	1	International card
	2	International card—alternate technology (EMV-compliant integrated circuit card containing VSDC applications)
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	National use only
	6	National use only—alternate technology (EMV-compliant integrated circuit card containing VSDC applications)
	7	Private cards—invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
2	0	Normal authorization
	1	Invalid for Visa card products
	2	Positive authorization mandatory
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Invalid for Visa card products
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
3	0	PIN required
	1	Normal verification
	2	Invalid for Visa card products
	3	Valid at ATMs only

Table A–10: Service Code Digit Value Descriptions (2 of 2)

Digit	Value	Description
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Prompt for PIN if PIN pad present
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products

A.5.2 Service Code Usage

Visa International occasionally assigns additional service codes as other uses are identified. An issuer, group of issuers, or country can apply to Visa International for the assignment of additional service codes for local, national, or international usage.

Table A–11: Valid Service Codes by Card Product

Service Code	Visa Credit, Debit, and Delta	Visa Electron	Interlink	Co-branded Visa Check and Interlink	Visa Travel Money	Plus ATM Only	Plus Co-branded with EFT Processor Marks
101	Valid			Valid			
106	Valid			Valid			
120		Valid[1]	Valid		Valid	Valid	Valid
121		Valid					
123						Valid	
126		Valid					
201	Valid						
206	Valid			Valid			
220						Valid	Valid
221		Valid					
223						Valid	
226		Valid					
501	Valid						
506	Valid						
520		Valid[1]					
521		Valid					
526		Valid					
601	Valid						
606	Valid						
621		Valid					
626		Valid					

[1] Service codes x21 and x26 are recommended for Visa Electron cards. Issuers who plan to use service code value x20 for Visa Electron cards should consult their Visa Customer Services representative.

Table A–12 describes the PIN Verification element encoded on Track 1 of the magnetic stripe.

Table A–12: Field 9—PIN Verification

Attributes	5 numerics
Description	Information needed to verify a PIN using the Visa PIN Verification Value (PVV)
Valid value	Numerics 0-9 Position 1: PIN Verification Key Index (PVKI) = 0 or 1-6 Position 2–5: PIN Verification Value (PVV)
Usage	The PIN verification data is required on Visa Gold/Premier cards. It is optional on other cards. If not required or needed, the field can be omitted from the stripe. If the issuer (BIN) uses the PIN Verification Service (PVS) for some, but not all issued cards, the PIN Verification field (both PVKI and PVV) should be zero-filled on those cards not using the PVS. If the issuer does not use the PVS for any cards in a card range, the zero-fill requirement is not needed. Refer to Chapter 6 for more information on the PVKI and PVV.

Table A–13 describes the discretionary data element encoded on Track 1 of the magnetic stripe.

Table A–13: Field 10—Discretionary Data

Attributes	8 to 10 alphanumerics
Description	Information that the issuer uses for on-us transactions and wants to have transmitted through the V.I.P. System for inquiries on interchange transactions. Visa Fleet Service Purchasing cards with a BIN range of 448450 to 448699 are required to use the last three positions of the discretionary data field to provide instructions for customized prompts.
Valid value	Any value in the character ranges 0–9 and A–Z, a space, a comma, or a slash (/). Visa Fleet Service Purchasing cards. Position 1: Reserved = 0 Position 2: Service Enhancement Indicator = 0, 1, or 2 Position 3: Service Prompt = 0, 1, 2, 3, 4, or 5
Usage	On Track 1, the length of this optional field is based on the lengths of the Cardholder Name field and on the presence or absence of the PIN Verification Data field and Fleet Service field. If the Cardholder Name field contains 26 characters (the maximum allowed), then positions 8, 11, 13, or 16 are available for discretionary data, as shown in Table A–14.

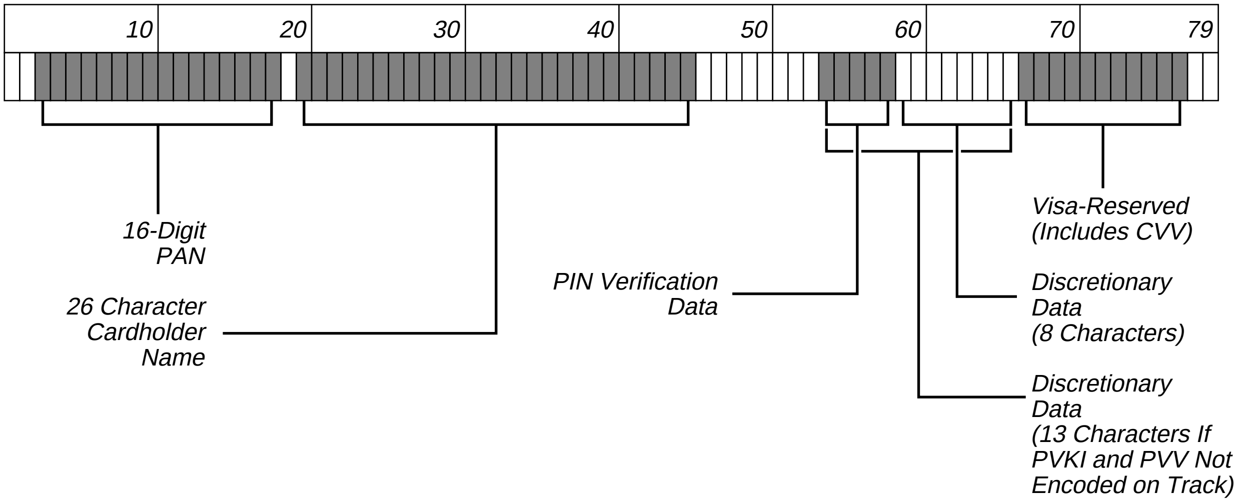
Table A–14 describes the matrix for the Discretionary data field encoded on Track 1 of the magnetic stripe.

Table A–14: Matrix for Discretionary Data Field

	PIN Verification length = 0	PIN Verification length = 5
16-digit PAN	13	8

Figure A–12 illustrates a 16-digit PAN, 26-position name, and 5-position PIN Verification field.

Figure A–12: PIN Verification Field


10
20
30
40
50
60
70
79
16-Digit PAN
26 Character Cardholder Name
PIN Verification Data
Visa-Reserved (Includes CVV)
Discretionary Data (8 Characters)
Discretionary Data (13 Characters If PVKI and PVV Not Encoded on Track)

When the Cardholder Name field contains fewer than 26 characters, the issuer can increase the length of the Discretionary Data field by the number of unused positions.

NOTE: *At the issuer's option, the Card Verification Value (CVV) located in the Visa-Reserved field can also be placed in the Discretionary Data field for ease of issuer verification.*

Table A–15 describes the Visa-Reserved data element encoded on Track 1 of the magnetic stripe.

Table A–15: Field 11—Visa-Reserved

Attributes	11 alphanumerics
Description	Last 11 positions of Track 1, excluding the End Sentinel and LRC character. Track 1 can vary in length depending on the presence or absence of the PIN Verification Data and Discretionary Data fields. The location of the last 1zeros1 positions of the track varies accordingly. See Figure A–3 through Figure A–6 for examples. This fixed-length, required field is used by Visa for the following subfields: • 11.1 Card Verification Value • 11.2 Authorization Control Indicator
Valid value	Positions 1–2: zeros Positions 3–5 (CVV): 3 numerics Position 7: zero Position 8 (ACI): A to Z or zero Positions 9–11: zeros

Table A–16 describes the CVV data element encoded on Track 1 of the magnetic stripe.

Table A–16: Field 11.1—Card Verification Value (CVV)

Attributes	3 numerics (positions 3–5 of the Visa-Reserved field)
Description	CVV is required on Track 1 of all Visa, Visa Electron, and Plus cards. Unique check value calculated from the data encoded in the stripe using a secure cryptographic process and a key known only to the issuer and Visa. Once encoded on the stripe, the CVV deters counterfeit card usage by validating encoded card information during the authorization process. The algorithm to calculate the CVV is described in Chapter 2 of this manual.
Valid value	0 to 9 When the CVV is first implemented, issuers using Visa verification to verify CVVs must supply Visa with the expiration date of the card series such that all cards expiring on or after this date are encoded with the CVV.

Table A–17 describes the Authorization Control Indicator data element encoded on Track 1 of the magnetic stripe.

Table A–17: Field 11.2—Authorization Control Indicator

Attributes	1 alphanumeric (position 8 of the Visa-Reserved field)
Description	Used for optional PCAS processing that describes the level of risk and the issuer's PIN policies associated with the cardholder. The risk levels reflect the best (lowest) risk to the worst (highest) risk, from A to D, respectively.
Valid value	Zero, C, Z, Y, or X. Use zero when an ACI code is not included. If the ACI code is included, select C, Z, Y, or X as appropriate for the risk level (see Table A–18).

Table A–18 describes the ACI data element encoded on Track 1 of the magnetic stripe.

Table A–18: ACI Values

ACI	Risk Level	PIN Policy
C	A	Optional
Z	B	Optional
Y	C	Optional
X	D	Optional

Table A–19 describes the End Sentinel data element encoded on Track 1 of the magnetic stripe.

Table A–19: Field 12—End Sentinel

Attributes	1 alphanumeric
Description	Character that follows the final character of data recorded on the track.
Valid value	?

Table A–20 describes the LRC data element encoded on Track 1 of the magnetic stripe.

Table A–20: Field 13—Longitudinal Redundancy Check (LRC)

Attributes	1 character
Description	Verification value that ensures that no data has been lost in the stripe-reading process. The LRC is equivalent to a check digit of the entire track, including the control characters.
Valid value	Any computed value
Usage	The LRC character is calculated using the following procedure: The value of each bit in the LRC character, excluding the parity bit, is defined such that the total count of “1” bits encoded in the corresponding bit location of all characters of the data message, including the Start Sentinel, data, End Sentinel, and LRC characters, is even. The parity bit in the LRC character is not a parity bit for the individual parity bits of the data message; it is the parity bit for the LRC character.

Track 2 Data B

This appendix describes Visa standards for the contents of Track 2 of the magnetic stripe and the magnetic stripe image on the integrated chip. Visa requirements conform to the International Organisation for Standardisation (ISO) standard 7811/2, *Identification Cards—Recording Technique—Part 2: Magnetic Stripe* and ISO standard 7813, *Identification Cards—Financial Transaction Cards*.

B.1 Track 2 Content Requirements

Requirements for the contents of a magnetic stripe conform to ISO 7813.

B.2 Record Format

Table B–1 displays the Track 2 record format. The maximum length of Track 2 is 40 characters, which must include the Start Sentinel, field separator, End Sentinel, and Longitudinal Redundancy Check (LRC).

Table B–1: Track 2 Record Format

Field Number	Length	Field Name
1[1]	1	Start Sentinel
2	12–19	Primary Account Number (PAN)
3	1	Separator
4	4	Card Expiration Date
5	3	Service Code
6	0 or 5	PIN Verification Data
7	varies[2]	Discretionary Data[3]
8[1]		End Sentinel
9[1]	1	Longitudinal Redundancy Check (LRC)

[1] Fields 1, 8 and 9 are not sent in online messages but are necessary for magnetic stripe-reading devices.

[2] The length depends on the lengths of fields 2 and 6. Refer to the Data Element Descriptions later in this appendix.

[3] Contains the 3-digit Card Verification Value (CVV) or optional iCVV on a chip.

B.3 Character Set

Table B–2 describes the Track 2 character set. This table corresponds to the character set table in ISO standard 7811/2, Section 10.1.3.

The hardware manufacturer specifies the data formats provided to an encoding machine. The encoding device must encode data characters using odd parity. Clocking bits for synchronization are not considered data.

An even-parity LRC character must be the last character in a track record.

NOTE: *bn = bit position number “n.” Table B–2: Track 2 Character Set.*

Table B–2: Track 2 Character Set

Char.	Hex	Binary				
		P	2^3	2^2	2^1	2^0
0	30	1	0	0	0	0
1	31	0	0	0	0	1
2	32	0	0	0	1	0
3	33	1	0	0	1	1
4	34	0	0	1	0	0
5	35	1	0	1	0	1
6	36	1	0	1	1	0
7	37	0	0	1	1	1
8	38	0	1	0	0	0
9	39	1	1	0	0	1
:	3A	1	1	0	1	0
;	3B	0	1	0	1	1
<	3C	1	1	1	0	0
=	3D	0	1	1	0	1
>	3E	0	1	1	1	0
?	3F	1	1	1	1	1

NOTE: *This coded character set is identical to the coded character set in ISO/ IEC 7811-4 and is derived from ASCII*

B.4 Encoding Examples

This section contains four examples of Track 2 encoding.

- Figure B–1 illustrates encoding the required fields without the PIN Verification Data field, but with the Discretionary Data field including the CVV in the first three positions of the field.
- Figure B–2 illustrates encoding with the PIN Verification Data field and the Discretionary Data field including the CVV in the first three positions of the field. This is an example of an Interlink mark appearing on a Visa debit card.
- Figure B–3 illustrates encoding without the PIN Verification Data field and with the Discretionary Data field containing only the CVV (remainder of the field is truncated). This example also contains an expiration date of December 2002.
- Figure B–4 illustrates encoding with the PIN Verification Data field and the Discretionary Data field containing issuer information in the first three positions of the field, followed by the CVV. This example represents a Track 2 using the maximum allowable position.

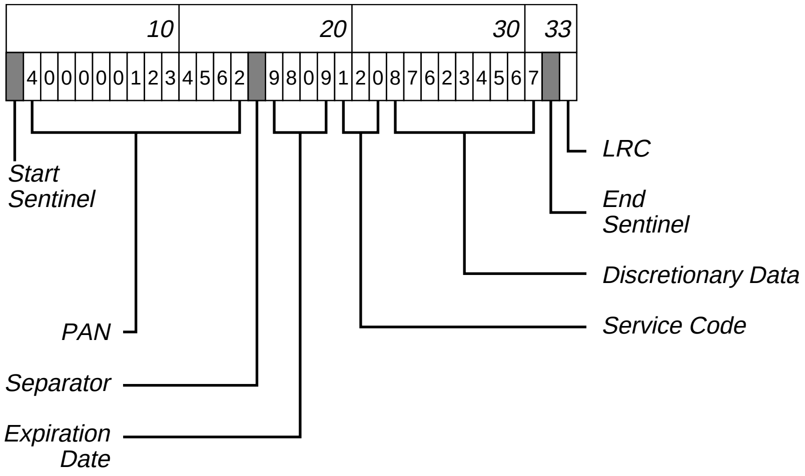
NOTE: *These examples provide a sample format only and should not be followed literally when encoding Track 2 of the magnetic stripe.*

B.4.1 Example 1: Encoding With Discretionary Data Field

Information to be encoded:

- PAN: 4000 0012 3456 2 (13 digits)
- Expiration Date: 09/98
- Service Code: 120
- PIN Verification Data: none
- Discretionary Data: 876234567 (first three positions = CVV)

Figure B–1: Encoding With Discretionary Data Field

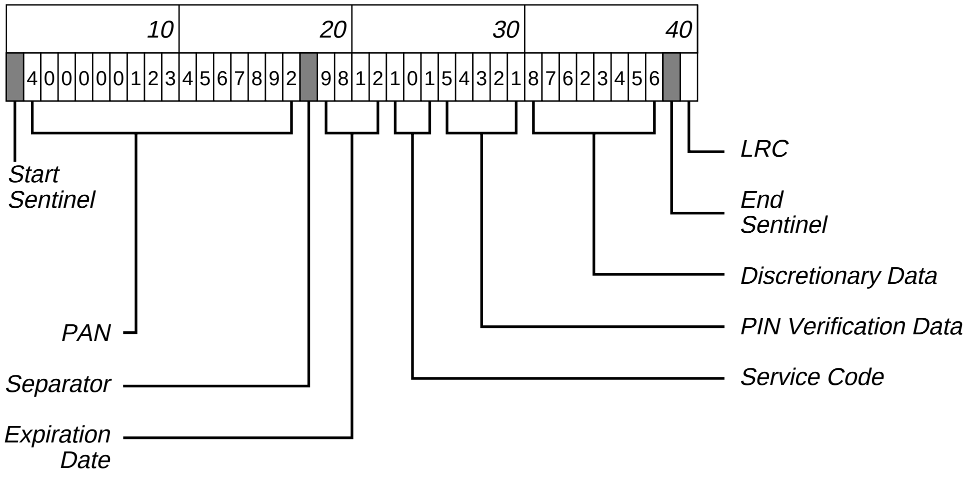


B.4.2 Example 2: Encoding With PIN Verification Data and Discretionary Data Fields

Information to be encoded:

- PAN: 4000 0012 3456 7892 (16 digits)
- Expiration Date: 12/98
- Service Code: 101
- PIN Verification Data: 5 (PVKI) and 4321 (PVV)
- Discretionary Data: 87623456 (first three positions = CVV)

Figure B–2: Encoding With PIN Verification and Discretionary Data

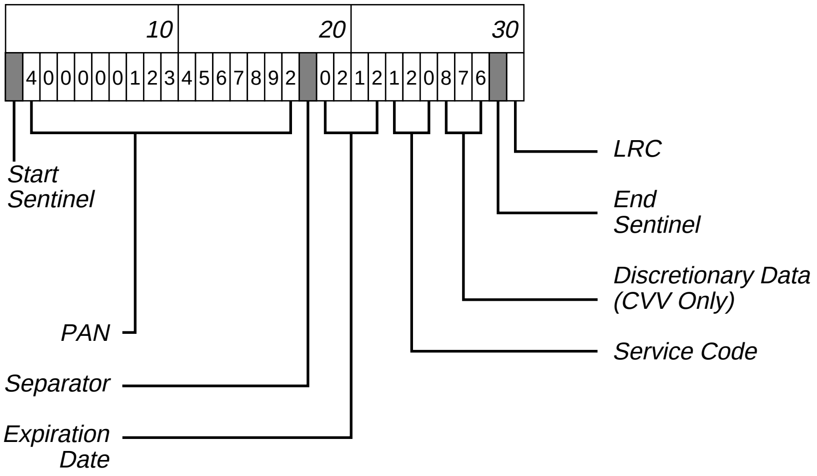


B.4.3 Example 3: Encoding With Discretionary Data Field (CVV Only)

Information to be encoded:

- PAN: 4000 0012 3456 7892 (16 digits)
- Expiration Date: 12/02
- Service Code: 120
- PIN Verification Data: none
- Discretionary Data: 876 (CVV only)

Figure B–3: Encoding With Discretionary Data

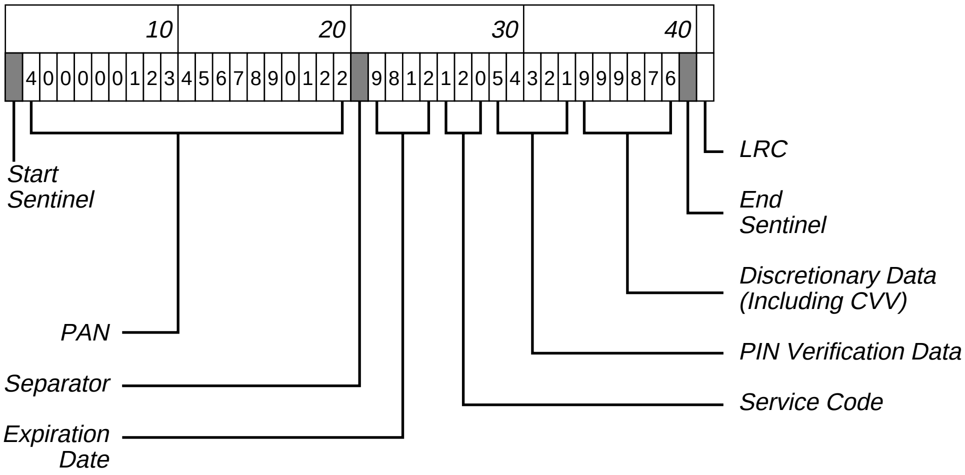


B.4.4 Example 4: Encoding With PIN Verification Data and Discretionary Data Fields

Information to be encoded:

- PAN: 4000 0012 3456 7890 122 (19 digits)
- Expiration Date: 12/98
- Service Code: 120
- PIN Verification Data: 5 (PVKI) and 4321 (PVV)
- Discretionary Data: 999876 (first three positions = issuer information; second three positions = DVV; remaining positions are truncated)

Figure B–4: Encoding With PIN Verification and Discretionary Data



B.5 Data Element Descriptions

This section describes the data elements encoded on Track 2. describes the Start Sentinel.

Table B–3: Field 1—Start Sentinel

Attributes	1 alphanumeric (numeric values only)
Description	Indicates the initial data position on the track.
Valid value	See Table B–1.

Table B–4 describes the PAN data element encoded on Track 2 of the magnetic stripe.

Table B–4: Field 2—Primary Account Number (PAN)

Attributes	12 to 19 numerics
Description	Cardholder account number with the last digit being a modulus-10-calculated digit
Valid value	Any valid ISO cardholder account number
Usage	When encoded on the magnetic stripe, the PAN must not include any spaces

Table B–5 describes the Separator data element encoded on Track 2 of the magnetic stripe.

NOTE: *Use of multiple separators may cause problems in some acquiring systems.*

Table B–5: Field 3—Separator

Attributes	1 alphanumeric
Description	Indicates the end of a variable-length field such as the PAN field. Only one separator is generally positioned on the track.
Valid value	See Table B–1.

Table B–6 describes the Card Expiration Date data element encoded on Track 2 of the magnetic stripe.

Table B–6: Field 4—Card Expiration Date

Attributes	4 numerics in the format YYMM
Description	Year and month after which the card can no longer be used
Valid value	YY must be 00 to 99 MM must be 01 to 12
Usage	The YYMM format follows ISO conventions for machine-processed dates. All cards with a Visa, Visa Electron, or Delta mark must have a finite expiration date that is no more than 20 years from the date of card issue.

Table B–7 describes the Service Code data element encoded on Track 2 of the magnetic stripe.

Table B–7: Field 5—Service Code

Attributes	3 numerics.
Description	A sequence of digits that, taken as a whole, is used to do the following: • Define various service attributes • Differentiate cards used in international or national interchange • Designate PIN requirements • Identify card restrictions
Valid value	The values allowed are made up of three individual digits: 1, 2, and 3. To be valid, each digit must be one of the acceptable values listed in Table B–8. These service code values apply to Visa card products (Visa, Plus, Visa Electron, Interlink, and Delta cards). Not all combinations of individually valid digit values result in a valid service code. Also, while a large number of service codes can be constructed from these values, only specific service codes are authorized for individual Visa card products. Table B–8 describes the service code values that are currently valid for Visa card products. Table B–9 and Table B–10 describe the preferred service codes by card product.

Table B–8 describes the Service Code Digit Value data element encoded on Track 2 of the magnetic stripe.

Table B–8: Service Code Digit Value Descriptions

Digit	Value	Description
1	0	Invalid for Visa card products
	1	International card
	2	International card—alternate technology (EMV-compliant integrated circuit card containing VSDC applications)
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	National use only
	6	National use only—alternate technology (EMV-compliant integrated circuit card containing VSDC applications)
	7	Private cards—invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
2	0	Normal authorization
	1	Invalid for Visa card products
	2	Positive authorization mandatory
	3	Invalid for Visa card products
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Invalid for Visa card products
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products
3	0	PIN required
	1	Normal verification
	2	Invalid for Visa card products.
	3	Valid at ATMs only
	4	Invalid for Visa card products
	5	Invalid for Visa card products
	6	Prompt for PIN if PIN pad present
	7	Invalid for Visa card products
	8	Invalid for Visa card products
	9	Invalid for Visa card products

B.5.1 Service Code Usage

Visa International occasionally assigns additional service codes as other uses are identified. An issuer, group of issuers, or country can apply to Visa International for the assignment of additional service codes for local, national, or international usage.

Table B–9: Valid Service Codes by Card Product

Service Code	Visa Credit, Debit, and Delta	Visa Electron	Interlink	Co-Branded Visa Check and Interlink	Visa Travel Money	Plus ATM Only	Plus Co-Branded With EFT Processor Marks
101	Valid			Valid			
106	Valid			Valid			
120		Valid[1]	Valid		Valid	Valid	Valid
121		Valid					
123						Valid	
126		Valid					
201	Valid						
206	Valid			Valid			
220						Valid	Valid
221		Valid					
223						Valid	
226		Valid					
501	Valid						
506	Valid						
520		Valid[1]					
521		Valid					
526		Valid					
601	Valid						
606	Valid						
621		Valid					
626		Valid					

[1] Service codes x21 and x26 are recommended for Visa Electron cards. Issuers who plan to use service code value x20 for Visa Electron cards should consult their Visa Customer Services representative.

Table B–10 describes the PIN Verification Data field encoded on Track 2 of the magnetic stripe.

Table B–10: Field 6—PIN Verification

Attributes	5 numerics
Description	Used to verify a PIN. Generally called Visa PVV or PIN offset value.
Valid value	Numerics 0 to 9 Position 1: PIN Verification Key Index (PVKI) = 0 or 1 to 6 Positions 2–5: PIN Verification Value (PVV)
Usage	The PIN Verification Data is required on Visa Gold/Premier cards. On other cards, it is optional depending upon the issuer's PIN verification process. If not required or needed, the field can be omitted from the stripe. If the issuer (BIN) uses the PIN Verification Service (PVS) for some, but not for all issued cards, the PIN Verification Data field (both PVKI and PVV) should be zero-filled on those cards not using the PVS. If the issuer does not use the PVS for any cards in a card range, the zero-fill requirement is not needed. For Visa Gold cards, the PVV must be encoded on both Track 1 and Track 2. Refer to Chapter 6 for more information on the PVKI and PVV.

Figure B–5 illustrates a 16-digit PAN, 26-position name, and 5-position PIN Verification field.

Figure B–5: PIN Verification Field

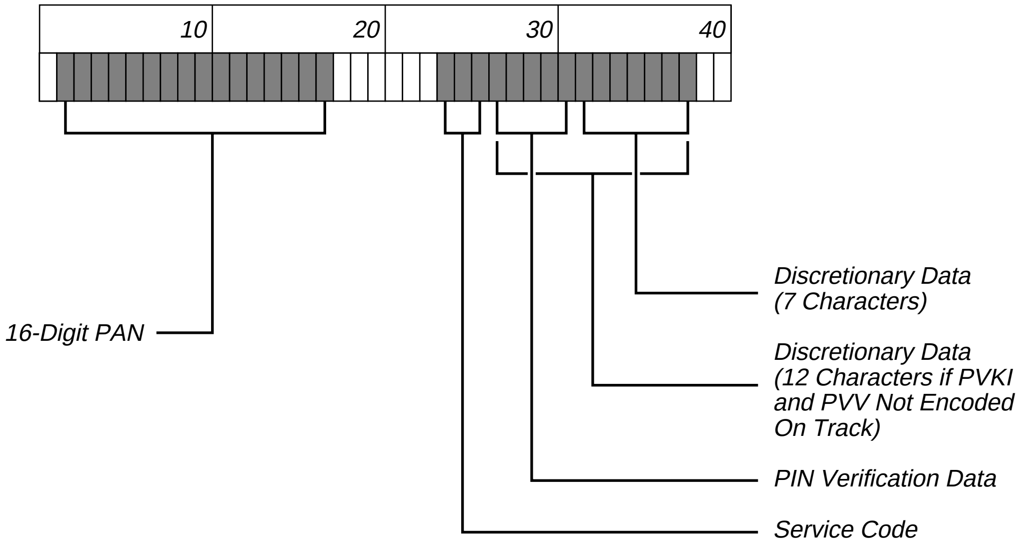


Table B–11 describes the Discretionary Data element encoded on Track 2 of the magnetic stripe.

Table B–11: Field 7—Discretionary Data (1 of 2)

Attributes	Up to 17 numerics; remaining digit positions can be three positions for CVV.
Description	Includes the Card Verification Value (CVV) plus any valid information that the issuer wants to have transmitted in the transactions. CVV is required on Track 2 of all Visa, Visa Electron, and Plus cards. iCVV is optional for chip.
Valid value	Any valid non-control or non-reserved character listed in Table B–1.

Table B–11: Field 7—Discretionary Data (2 of 2)

Usage	On Track 2, the maximum length of this optional field is based on the length of the Primary Account Number (PAN) and on the presence or absence of the PIN Verification field. Because Discretionary Data fields are optional, they should not be filled with pad characters solely with the intent to fill all positions on Track 2. The 3-digit CVV must be encoded in the Discretionary Data field. While Visa recommends placing the CVV at the start of this field, any three contiguous positions can be used. Figure B–6 illustrates the recommended placement of the CVV in an 8-digit Discretionary Data field. iCVV is optional for chip. ***Note:*** *If Visa is to provide CVV validation for an issuer, the issuer must provide Visa with the location of the CVV on Track 2 for verification purposes. The issuer describes the location by giving its displacement from the end of the Service Code field. For example, in Figure B–6, the displacement is 5. If the PIN Verification field was not encoded on the stripe, the displacement would be 0. For details on calculating the Track 2 CVV, refer to Chapter 2.*

Figure B–6: Discretionary Data Field

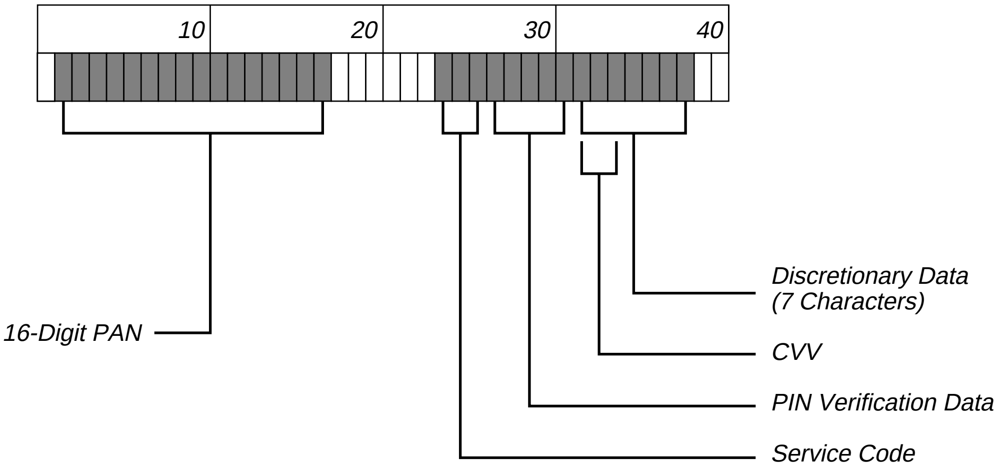


Table B–12 describes the End Sentinel element encoded on Track 2 of the magnetic stripe.

Table B–12: Field 8—End Sentinel

Attributes	1 alphanumeric
Description	Indicates the final data position on the track.
Valid value	See Table B–1.

Table B–13 describes the Longitudinal Redundancy Check element encoded on Track 2 of the magnetic stripe.

Table B–13: Field 9—Longitudinal Redundancy Check (LRC)

Attributes	1 digit 0 to F
Description	Verification value that ensures that no data has been lost in the stripe-reading process. The LRC is equivalent to a check digit of the entire track including the control characters.
Valid value	Any computed value
Usage	The LRC character is calculated using the following procedure: • The value of each bit in the LRC character, excluding the parity bit, is defined such that the total count of “1” bits encoded in the corresponding bit location of all characters of the data message, including the Start Sentinel, data, End Sentinel, and LRC characters, is even. • The parity bit in the LRC character is not a parity bit for the individual parity bits of the data message: it is the parity bit for the LRC character.

Exclusive-OR Operation (XOR) C

The exclusive-OR (XOR) logic operation is also known as Mod 2 Addition or Binary Addition Without Carry. Executing the XOR operation for each combination of two corresponding bits results in the following:

0	0	1	1
XOR 0	XOR 1	XOR 0	XOR 1
0	1	1	0

The following example illustrates the XOR operation on a sample set of hexadecimal values. The sample parallels applying the XOR logic operation to three ZCMK components as discussed in Chapter 7, DES Key Management.

Assume the following hexadecimal values:

First Value:	F1	73
Second Value:	29	C1
Third Values:	49	5E

Using binary notation, these values are represented as follows. Refer to Figure C–1.

First Value:	1111	0001	0111	0011	(F1	73)
Second Value:	0010	1001	1100	0001	(29	C1)
Third Values:	0100	1001	0101	1110	(49	5E)

Table C–1: Binary to Hexadecimal Conversion

Binary = Hexadecimal	Binary = Hexadecimal
0000 = 0	1000 = 8
0001 = 1	1001 = 9
0010 = 2	1010 = A
0011 = 3	1011 = B
0100 = 4	1100 = C
0101 = 5	1101 = D
0110 = 6	1110 = E
0111 = 7	1111 = F

When applied to the first two values, the XOR operation yields the following intermediate result:

First Value:	1111	0001	0111	0011	(F1	73)
XOR						
Second Value:	0010	1001	1100	0001	(29	C1)
Intermediate Result:	1101	1000	1011	0010	(D8	B2)

When the intermediate result is XOR'd with the third value, the final result is as follows.

Intermediate Result:	1101	1000	1011	0010	(D8	B2)
XOR						
Third Value:	0100	1001	0101	1110	(49	5E)
Final Result:	1001	0001	1110	1100	(91	EC)

Like any form of addition, the XOR operation produces the same result regardless of the order in which the components are combined.

Most computers support the XOR instruction. For those that do not, the XOR operation can be implemented with a table look-up procedure.

An advantage of separating a key into three XOR components instead of, for example, the first X bits, the middle Y bits, and the last Z bits, is that knowing one, or even two, of the key components provides no more information about the key than knowing none of the components

Master Forms D

This appendix contains the master forms used for key management activities.

D.1 Key Management Forms

Key management activities related to Zone Control Master Keys (ZCMK) and member working keys require the use of forms contained in this appendix. The key management forms include:

- Visa Key Management Request
- Designation of Key Custodians
- Key Conveyance for Translation of Working Keys
- Key Conveyance Form for Master Derivation Key

The procedures that use these forms are described in Chapter 7, DES Key Management. When a procedure requires the use of a form, the member duplicates the master from this appendix.

D.1.1 Visa Key Management Request

The Visa Key Management Request form is required when a member requests a key management service from Visa, which includes a request for one or more of the following:

- Generation of a ZCMK
- Generation of member working keys
- Translation of member-generated working keys

D.1.2 Designation of Key Custodians

The Designation of Key Custodians form is used to specify the three persons who are to receive the cleartext components of a ZCMK.

Upon receipt of this form, Visa generates a ZCMK for the member in the form of three cleartext components, and mails one of the components to each Key Custodian identified on the form. Visa includes the key-check value for the ZCMK with each of the components.

This form must accompany the Visa Key Management Request Form whenever a member requests Visa to generate a ZCMK.

D.1.3 Key Conveyance for Translation of Working Keys

The Key Conveyance for Translation of Working Keys is used to convey keys to or from Visa that are encrypted by the ZCMK. This includes the AWK, IWK, PVK, CVK, CVK2, CAK, and MDK.

D.1.4 Key Conveyance Form for Master Derivation Key

The Key Conveyance Form for Master Derivation Key is used to convey one or more member-generated MDK keys to Visa.

The form is used whenever a member requests Visa to implement new MDK keys.

Visa Key Management Request Form (1 of 2)

VISA KEY MANAGEMENT REQUEST FORM- Page One

Instructions: For a Zone Control Master Key (ZCMK) request, attach the Designation of Key Custodians. For ***translation*** of new working keys, attach the appropriate Key Conveyance Form(s).

Requester Identification and Authorization

Member Name: ____

Processing Center BIN: ______________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ____
(Please type name and title)

Address: ____
____
____

Contact Numbers ______________________(telephone)______________________(fax)

Signature Date

Activation Date for Keys: ______________________

Zone Control Master Key (ZCMK)

[ ] Create a new ZCMK [ ] Single Length [ ] Double Length

Working Keys

ZCMK Creation Date: ______________________ ZCMK Key-Check Value: ___ ___ ___ ___ ___ ___

Type of Request: [ ] Original [ ] Replacement [ ] Additional

[ ] Create the following Working Keys:

		Set Index 1	Set Index 2	Single-Length	Double-Length
[ ] Acquirer Working Key(s)	(AWK)	[ ]	[ ]	[ ]	[ ]
[ ] Issuer Working Key(s)	(IWK)	[ ]	[ ]	[ ]	[ ]
[ ] PIN Verification Pair(s)	(PVK)	[ ]	[ ]	Up to six pairs available	
[ ] Card Verification Pair(s)	(CVK)	[ ]	[ ]		
[ ] Card Verification 2 Pair(s)	(CVK2)	[ ]	[ ]		
[ ] Cardholder Auth. Verif. Key Pair(s)	(CAK)	[ ]	[ ]		
[ ] IBM DES PIN Verification Key			(IBM DES)		
[ ] Atalla PIN Verification			(Atalla)		
[ ] Master Derivation Keys			(MDK	Up to 24	
[ ] Acquirer Dynamic Key Exchange Key			(AKEK)		
[ ] Issuer Dynamic Key Exchange Key			(IKEK)		
[ ] MAC Sending Key Exchange Key			(SKEK)		
[ ] MAC Receiving Key Exchange Key			(RKEK)		
[ ] Visa Cash CEPS Static Acquirer Key Exchange Key			(AKEK)		
[ ] Visa Cash CEPS Static Issuer Key Exchange Key			(IKEK)		

Visa Key Management Request Form (2 of 2)

VISA KEY MANAGEMENT REQUEST FORM- Page Two

Working Keys

[ ] Translate the following Working Keys:

[ ] AWK	[ ] IWK	[ ] PVK	[ ] CVK	[ ] CVK2
[ ] CAK	[ ] IBM DES	[ ] Atalla	[ ] MDK	

Designation of Key Custodians

DESIGNATION OF KEY CUSTODIANS

Instructions: Please type or print ***clearly*** all information. Use **ONLY** street addresses for designated custodians.

Requester Identification and Authorization

□ Copy from Request Form

Member Name: ____

Processing Center BIN: ______________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ____

(Please type name and title,)

Address: ____
____
____

Contact Numbers ________________________(telephone)____________________________________(fax)

Signature Date

Custodian One

Custodian Name & Title: ____

Address: ____
____
____

Custodian Two

Custodian Name & Title: ____

Address: ____
____
____

Custodian Three

Custodian Name & Title: ____

Address: ____
____
____

Key Conveyance Form for Translation of Working Keys (1 of 5)

KEY CONVEYANCE FORM FOR TRANSLATION OF WORKING KEYS (Page One)

Instructions: **ALL** keys entered on the following pages ***must*** be encrypted.

Requester Identification and Authorization

□ Copy from Request Form

Member Name: ____

Processing Center BIN: ____________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ____

(Please type name and title)

Address: ____
____
____

Contact Numbers ____________________(telephone)____________________(fax)

Signature Date

Acquirer Working Key(s) – AWK

AWK Zone Key Index = 1 [ ] Single-Length [ ] Double-Length

AWK ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

AWK Zone Key Index = 2 [ ] Single-Length [ ] Double-Length

AWK ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Issuer Working Key(s) – IWK

IWK Zone Key Index = 1 [ ] Single-Length [ ] Double-Length

IWK ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

IWK Zone Key Index = 2 [ ] Single-Length [ ] Double-Length

IWK ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Key Conveyance Form for Translation of Working Keys (2 of 5)

KEY CONVEYANCE FORM FOR TRANSLATION OF WORKING KEYS (Page Two)

Instructions: **ALL** keys entered on the following pages ***must*** be encrypted.

Requester Identification and Authorization

□ Copy from Request Form

Member Name: ______________________________

Processing Center BIN: ____________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ______________________________

(Please type name and title,)

Address: ______________________________
____
____

Contact Numbers ____________________(telephone)____________________(fax)

Signature Date

PIN Verification Key – (PVK)—PVV ***Both keys for PAIR are REQUIRED***

PVK1 = 1 PVKA ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyA Check Value ___ ___ ___ ___ ___ ___
PVKB ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyB Check Value ___ ___ ___ ___ ___ ___

PVK1 = 2 PVKA ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyA Check Value ___ ___ ___ ___ ___ ___
PVKB ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyB Check Value ___ ___ ___ ___ ___ ___

PVK1 = 3 PVKA ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyA Check Value ___ ___ ___ ___ ___ ___
PVKB ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyB Check Value ___ ___ ___ ___ ___ ___

PVK1 = 4 PVKA ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyA Check Value ___ ___ ___ ___ ___ ___
PVKB ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyB Check Value ___ ___ ___ ___ ___ ___

PVK1 = 5 PVKA ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyA Check Value ___ ___ ___ ___ ___ ___
PVKB ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyB Check Value ___ ___ ___ ___ ___ ___

PVK1 = 6 PVKA ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyA Check Value ___ ___ ___ ___ ___ ___
PVKB ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
KeyB Check Value ___ ___ ___ ___ ___ ___

Key Conveyance Form for Translation of Working Keys (3 of 5)

KEY CONVEYANCE FORM FOR TRANSLATION OF WORKING KEYS (Page Three)

Instructions: **ALL** keys entered on the following pages ***must*** be encrypted.

Requester Identification and Authorization

□ Copy from Request Form

Member Name: ____

Processing Center BIN: ____________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ____

(Please type name and title,)

Address: ____

____

____

Contact Numbers ________________________(telephone)__________________________________(fax)

Signature Date

Card Verification Key – (CVK)–CVV ***Both keys for PAIR are REQUIRED***

CVK Pair 1

CVK Key A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key A–Key Check Value_ __ ___ ___ ___ ___ ___

CVK Key B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key B–Key Check Value_ __ ___ ___ ___ ___ ___

CVK Pair 2

CVK Key A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key A–Key Check Value_ __ ___ ___ ___ ___ ___

CVK Key B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key B–Key Check Value_ __ ___ ___ ___ ___ ___

Card Verification Keys 2– (CVK2)–CVV2 ***Both keys for PAIR are REQUIRED***

CVK2 Pair 1

CVK2 Key A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key A–Key Check Value_ __ ___ ___ ___ ___ ___

CVK2 Key B___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key B–Key Check Value_ __ ___ ___ ___ ___ ___

CVK2 Pair 2

CVK2 Key A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key A–Key Check Value_ __ ___ ___ ___ ___ ___

CVK2 Key B___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key B–Key Check Value_ __ ___ ___ ___ ___ ___

Key Conveyance Form for Translation of Working Keys (4 of 5)

KEY CONVEYANCE FORM FOR TRANSLATION OF WORKING KEYS (Page Four)

Instructions: **ALL** keys entered on the following pages ***must*** be encrypted.

Requester Identification and Authorization

□ Copy from Request Form

Member Name: ____

Processing Center BIN: ____________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ____

(Please type name and title,)

Address: ____
____
____

Contact Numbers ______________________(telephone)________________________________(fax)

Signature Date

1. Please identify the Access Control Server (ACS) performing the CAVV calculation for this BIN
   Visa □
   Other □

2. Should VisaNet forwarded this Key Conveyance Form to the Visa ACS?
   Yes □
   No □

3. Please identify the intent of this Key Conveyance Form
   Inital BIN Set-Up □
   Replace CAK Pair 1 □
   Replace CAK Pair 2 □
   Replace Both CAK Pairs □

Cardholder Authentication Key – (CAK)–CAVV ***Both keys for PAIR are REQUIRED***

CAK Pair 1

CAK Key A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key A–Key Check Value_ __ ___ ___ ___ ___ ___

CAK Key B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key B–Key Check Value_ __ ___ ___ ___ ___ ___

CAK Pair 2

CAK Key A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key A–Key Check Value_ __ ___ ___ ___ ___ ___

CAK Key B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key B–Key Check Value_ __ ___ ___ ___ ___ ___

Key Conveyance Form for Translation of Working Keys (5 of 5)

KEY CONVEYANCE FORM FOR TRANSLATION OF WORKING KEYS (Page Five)

Instructions: **ALL** keys entered on the following pages ***must*** be encrypted.

Requester Identification and Authorization

□ Copy from Request Form

Member Name: ____

Processing Center BIN: ____________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ____

(Please type name and title,)

Address: ____
____
____

Contact Numbers ____________________(telephone)____________________(fax)

Signature Date

IBM DES PIN Verification Key – IBM DES

IBM DES Key ____

Check Value ____________________

Atalla PIN Verification Key – Atalla

PVKA ____

Key Check Value ____________________

Variant applied to Key [ ] Yes [ ] No

PVKB ____

Key Check Value ____________________

Variant applied to Key [ ] Yes [ ] No

Key Conveyance Form for Master Derivation Key (1 of 6)

KEY CONVEYANCE FORM FOR MASTER DERIVATION KEY

Instructions: **ALL** keys entered on the following pages ***must*** be encrypted.

Requester Identification and Authorization

□ Copy from Request Form

Member Name: ______________________________

Processing Center BIN: ____________________ Network: Credit / SMS (circle one)
(Storage BIN for ZCMK & Working Keys)

Submitted by: ______________________________

(Please type name and title,)

Address: ______________________________
____
____

Contact Numbers ____________________(telephone)____________________(fax)

Signature Date

MASTER DERIVATION KEY– MDK (ALL KEYS ARE DOUBLE-LENGTH KEYS (1 of 6)

Derivation Key Index ____________ Replaces Derivation Key Index ____________

MDK 1 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ____________ Replaces Derivation Key Index ____________

MDK 2 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ____________ Replaces Derivation Key Index ____________

MDK 3 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___
B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single( ) Double

Key Conveyance Form for Master Derivation Key (2 of 6)

MASTER DERIVATION KEY– MDK (ALL KEYS ARE DOUBLE-LENGTH KEYS (2 of 6)

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 4 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 5 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 6 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 7 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 8 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Key Conveyance Form for Master Derivation Key (3 of 6)

MASTER DERIVATION KEY– MDK (ALL KEYS ARE DOUBLE-LENGTH KEYS (3 of 6)

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 9 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 10 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 11 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 12 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 13 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Key Conveyance Form for Master Derivation Key (4 of 6)

MASTER DERIVATION KEY– MDK (ALL KEYS ARE DOUBLE-LENGTH KEYS (4 of 6)

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 14 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 15 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 16 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 17 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 18 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Key Conveyance Form for Master Derivation Key (5 of 6)

MASTER DERIVATION KEY– MDK (ALL KEYS ARE DOUBLE-LENGTH KEYS (5 of 6)

Derivation Key Index ______________ Replaces Derivation Key Index ______________

MDK 19 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ______________ Replaces Derivation Key Index ______________

MDK 20 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ______________ Replaces Derivation Key Index ______________

MDK 21 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ______________ Replaces Derivation Key Index ______________

MDK 22 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Derivation Key Index ______________ Replaces Derivation Key Index ______________

MDK 23 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Key Conveyance Form for Master Derivation Key (6 of 6)

MASTER DERIVATION KEY– MDK (ALL KEYS ARE DOUBLE-LENGTH KEYS (6 of 6)

Derivation Key Index ________________ Replaces Derivation Key Index ______________

MDK 24 A ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

B ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

Key Check Value ___ ___ ___ ___ ___ ___

Online UDK ( ) Single ( ) Double

Glossary

acceptance mark

A mark that denotes point-of-transaction acceptance for payment under specific rules.

account number

A primary cardholder account number that is displayed and encoded on a Visa or Visa Electron card or proprietary card bearing the Plus symbol.

account number verification

A process by which a member or its authorizing processor determines if there is negative information on an account number in the exception file for transactions that do not require authorization.

acquirer

A 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.

ATM

An unattended terminal that has electronic capability, accepts PINs, and disburses currency or cheques.

ATM acquirer

An acquirer that provides ATM services.

ATM cash disbursement

A cash disbursement obtained at an ATM that displays the Visa, Visa Electron or Plus acceptance mark for which the cardholder's PIN is accepted.

authorization

A process, as specified in the Visa International Operating Regulations, where an issuer, authorizing processor, or stand-in processing approves a transaction. The process includes domestic and international authorization.

authorizing processor

A processor that provides authorization services for merchants or other members.

automated dispensing machine

An unattended terminal that accepts payment for dispensed goods (such as fuel), has electronic capability, and accepts PINs, but does not disburse currency.

blocking

The action taken by a point-of-transaction terminal or acquirer host processing system that prevents the acceptance of cards containing service code values that are not recognized.

card

A valid Visa or Visa Electron card or a proprietary card that bears the Plus symbol.

Card Verification Value (CVV)

A unique check value encoded on the magnetic stripe of a card to validate card information during the authorization process. The Card Verification Value is calculated from the data encoded on the magnetic stripe using a secure cryptographic process.

Card Verification Value 2 (CVV2)

A unique check value generated using a secure cryptographic process, as specified in the VisaNet manuals, that may be indent-printed on the back of a Visa card. Card Verification Value 2 is designed to reduce fraud losses on transactions when the card is not present, such as Mail Order/Telephone Order (MOTO) and electronic commerce transactions, and to augment the effectiveness of voice referrals.

cardholder

An individual to whom a card is issued or who is authorized to use the card.

cash disbursement

Currency, including travelers cheques, paid out to a cardholder using a card.

chargeback

A transaction that an issuer returns to an acquirer.

cheque

A travelers cheque that a member issues that bears the Visa-owned marks.

chip

An electronic component designed to perform processing or memory functions.

chip card

A card embedded with an integrated circuit chip that communicates information to a point-of-transaction terminal.

chip device

A point-of-transaction terminal capable of reading, communicating, and processing transaction data from an integrated circuit card.

clearing record

A record of a presentment, chargeback, representment, or reversal in the format necessary to clear the transaction.

cleartext

Information in a form that can be read by humans.

ciphertext

The result of enciphering cleartext with an encryption algorithm under a secret key.

cryptographic key

See DES Key.

CVV

See Card Verification Value (CVV).

CVV2

See Card Verification Value 2 (CVV2).

data capture-only capability

Point-of-transaction capability whereby the transaction receipt data is electronically captured for deposit purposes but does not have the capability to go online.

deposit

The submission of a transaction receipt by a merchant to an acquirer that results in a credit or debit to the merchant's Visa account.

Data Encryption Algorithm (DEA)

The algorithm used to implement the Data Encryption Standard. This algorithm was derived from the IBM Lucifer encryption algorithm.

Data Encryption Standard (DES)

The symmetric key methodology defined in ANSI X.9.77. This is the only method approved for encrypting PINs in Visa card product transactions.

Derived Unique Key Per Transaction (DUKPT)

Every PIN entered at a specific PED is encrypted under a unique derivation key.

DES Key

A series of secret hexadecimal values used to encrypt or decrypt confidential information.

editing

Execution of logic within a terminal or host system that examines the service code, expiration date value, or both, against predefined criteria, such as a list of known service codes or the current calendar date.

electronic transaction receipt

A transaction receipt whereby the terminal generates the required data that is printed on the transaction receipt.

exception file

A VisaNet file of account numbers for which the issuer has predetermined an authorization response that a member accesses online.

expired card

A card on which the embossed, encoded, or printed expiration date has passed.

face-to-face environment

An environment whereby a transaction is completed under the following conditions: card is present, cardholder is present, and the individual representing the merchant or acquirer completes the transaction.

iCVV

An optional VSDC risk control feature that detects chip data being copied and being used to counterfeit magnetic stripe card transactions.

interchange

The exchange of clearing records between members. The *Visa International Operating Regulations* refers to domestic and international interchange.

international board

The Visa International Board of Directors.

International Organisation for Standardisation (ISO)

The specialized international agency that establishes and publishes international technical standards.

invalid service code value

Case 1: The service code value encoded on the magnetic stripe is not valid for that card product. For example, service code 120 is not valid for any card bearing a Visa mark.

Case 2: The service code does not allow the transaction being attempted, such as an attempt to use a card requiring online authorization at a terminal incapable of operating online.

issuer

A member that issues Visa cards, Visa Electron cards, or proprietary cards that bear the Plus symbol and 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.

Key Exchange Key (KEK)

A key used to encrypt other keys for conveyance between devices. For example, unique session keys conveyed from a host to network endpoints such as PIN pads attached to POS devices would be encrypted under a KEK.

key management service

A service that Visa provides to process, store, and transmit member keys associated with the security algorithm used in the V.I.P. System to protect the security of PINs.

magnetic stripe

The stripe on a card that contains the necessary information to complete a transaction.

magnetic strip terminal

A terminal that can read the magnetic stripe on a card.

manual cash disbursement

A cash disbursement obtained with a Visa or Visa Electron card in a face-to-face environment.

mark

A word, name, design, symbol, other device, or any combination thereof that an entity adopts to identify its goods or services.

member

An entity that is a member of Visa. Refer to the *Visa International Operating Regulations* for information about the different types of members.

merchant

An entity that contracts with an acquirer to originate transactions and that displays the Visa symbol, Visa Electron symbol, or both. Refer to the *Visa International Operating Regulations* for information about the different types of merchants.

Master Derivation Key (MDK)

The master key used for the VSDC cryptogram processing associated with card authentication, issuer authentication, and dispute processing.

normal authorization

The transaction must be authorized according to the rules governing the particular point of transaction.

online

A method of requesting an authorization through a communications network other than voice to one of the following: an issuer an authorizing processor stand-in processing.

online authorization

Authorization requests that are processed through a communications network (other than voice) to the issuer, the issuer's authorizing processor or the V.I.P.

System stand-in function operating on behalf of the issuer. Note that an online terminal must operate as an offline terminal when experiencing communications failures.

online terminal

A point-of-transaction device that routes all transactions online for issuer authorization.

on-us transaction

A transaction in which the issuer and the acquirer are the same.

PIN

A personal identification code that identifies a cardholder in an authorization request that originates at a terminal with authorization-only or data capture-only capability. A PIN may be alphabetic, numeric, or a combination of both.

PIN Entry Device (PED)

A keypad, laid out in a prescribed format, combined with electronic components housed in a tamper-resistant or tamper-evident shell that can capture and encrypt cardholder PINs.

PIN pad

See PIN Entry Device (PED).

PIN verification

A procedure used to verify the cardholder's identity when a PIN is used in an authorization request.

PIN verification field

A field encoded on the magnetic stripe that is comprised of a PIN verification value that is calculated with an algorithm, which uses portions of the account number, PIN, and a one-digit key indicator.

PIN verification service

A service that Visa provides for the verification of cardholder PINs that are transmitted with authorization requests.

PIN Verification Value (PVV)

A cryptographic representation of a cardholder PIN that can be used to verify the correctness of a PIN entered at the point of transaction.

PIN verification value file

A VisaNet file of account numbers and PIN verification values that is maintained at a VisaNet Interchange Center for use as part of the PIN verification service. The PVV is maintained at the issuer's option.

PLUS symbol

An ATM acceptance mark that is comprised of the PLUS design combined with the PLUS wordmark that denotes ATM access only. One of the PLUS program marks.

point of sale

See point of transaction.

point of service

See point of transaction.

point of transaction

The physical location at which a merchant or acquirer (in a face-to-face environment) or an unattended terminal (in an unattended environment) completes a transaction receipt.

point-of-transaction capability

The capability of a merchant, acquirer, or unattended terminal to obtain an authorization and process transaction receipt data. The *Visa International Operating Regulations* refer to the following point of transaction capability types: authorization-only capability data, capture-only capability, electronic capability, manual capability, and semi-electronic capability.

point of transaction terminal

A device used at the point of transaction that has a corresponding point of transaction capability. The *Visa International Operating Regulations* refers to the following types of point of transaction terminals: ATM automated dispensing machine integrated circuit card terminal, limited-amount terminal, magnetic stripe telephone, magnetic stripe terminal, self-service terminal.

Positive Cardholder Authorization Service

A set of risk control services available to issuers as specified in the VisaNet manuals.

positive verification

The process of identifying the cardholder through the use of a PIN. When verified, the PIN is a substitute for the cardholder's signature.

presentment

A clearing record that an acquirer presents to an issuer through interchange either initially (a first presentment) or after a chargeback (a representment).

processor

A member, Visa, or a Visa-approved nonmember acting as the agent of a member, that provides authorization, clearing, or settlement services for merchants and members. The *Visa International Operating Regulations* refers to the following types of processors: authorizing processor, auto-Telex user clearing processor, manual authorizer, V.I.P. system user.

proprietary card

A card that does not bear a Visa or Visa Electron symbol.

PVV

See PIN Verification Value (PVV).

representment

A clearing record that an acquirer presents to an issuer through interchange after a chargeback.

retail transaction

A transaction at a retail merchant outlet.

reversal

A BASE II or online financial transaction used to negate or cancel a transaction that has been sent through interchange in error.

service code

A number encoded on the magnetic stripe that identifies the circumstances under which the encoded BIN is valid. For example, international transactions, domestic transactions, restricted card use, or local services.

stand-in processing (STIP)

The V.I.P. system component that provides authorization services on behalf of an issuer when the Positive Cardholder Authorization System is used or when the issuer or its authorizing processor is unavailable.

terminal

See point of transaction terminal.

transaction

The act between a cardholder and a merchant or an acquirer that results in the generation of a transaction receipt. The *Visa International Operating Regulations* refers to the following types of transactions: advance lodging, deposit ATM, cash disbursement, cash disbursement deferred, clearing delayed, delivery domestic emergency cash disbursement, emergency cheque refund, fee collection international interregional intraregional mail/ home order, manual cash disbursement, no-show online financial prepaid card priority, check-out quasi-cash, recurring retail, T&E telephone service, VisaPhone wire transfer.

transaction receipt

An electronic or paper record of a transaction (or a copy), generated at the point-of-transaction.

The *Visa International Operating Regulations* refers to the following types of transaction receipts: cash disbursement, counterfeit credit domestic, electronic exported guest folio, international airline, international interregional sales draft substitute, T&E document transaction record.

unattended terminal

A device that reads, captures, and transmits card information. A cardholder operates this device in an unattended environment. The *Visa International Operating Regulations* refers to the following types of unattended terminals: ATM automated dispensing machine, cardholder-activated terminal, limited-amount terminal, self-service terminal.

unrecognized service code

A service code that a magnetic stripe terminal cannot recognize.

Visa card

A card that bears the Visa symbol, which enables a Visa cardholder to obtain goods, services, or cash from a Visa merchant or an acquirer. A Visa card is always one of the following: Visa Business card, Visa Classic card, Visa Gold card, Visa Premier card, Visa Purchasing card.

VisaNet Integrated Payment (V.I.P.) System

VisaNet Integrated Payment System is the primary system for processing all online VisaNet authorization and financial request transactions. V.I.P. supports both dual message and single message processing. In both cases, settlement occurs separately. It is composed of the Common Interface Function and two basic components; the BASE I component and the Single Message System (SMS) component.

Visa Smart Debit/Visa Smart Credit (VSDC)

The introduction of an integrated circuit chip to the traditional Visa credit and debit products. The additional functionality of the chip allows for new risk management processing between the card and terminal at the point-of-transaction. The new processing enables more secure offline and online transactions aiding members in their authorization decision and dispute processing.

zero-floor limit

A floor limit with a currency amount of zero, which means that authorization is required for all transactions.

Zone Control Master Key

A master key used to encrypt working keys conveyed between nodes on a network. Visa generates and conveys ZCMKs to all members and processors connected to VisaNet.

Index