SET Secure Electronic Transaction Specification

Book 1: Business Description

Version 1.0
May 31, 1997

PC

Preface

Introduction

The development of electronic commerce is at a critical juncture.

- Consumer demand for secure access to electronic shopping and other services is very high.
- Merchants want simple, cost-effective methods for conducting electronic transactions.
- Financial institutions want a level playing field for software suppliers to ensure quality products at competitive prices.
- Payment card brands must be able to differentiate electronic commerce transactions without significant impact to the existing infrastructure.

The next step toward achieving secure, cost-effective, on-line transactions to satisfy market demand is the development of a single, open industry specification.

Secure Electronic Transaction protocol

Visa and MasterCard have jointly developed the SET Secure Electronic Transaction protocol as a method to secure payment card transactions over open networks. SET is being published as an open specification for the industry. This specification is available to be applied to any payment service and may be used by software vendors to develop applications.

Advice and assistance in the development of this specification have been provided by GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa, and VeriSign.

Purpose

This document contains background information and processing flows for the SET Secure Electronic Transaction protocol.

Audience

It is intended as an introduction to SET for anyone interested in the processing of payment card transactions on electronic networks, including vendors developing software that will interoperate with implementations of SET from other vendors.

For more Information

Many vendors will have developed software that either interfaces with payment systems or uses public-key cryptography, but few will have done both. The introductory material is only intended to be a primer on these topics. Readers are encouraged to study additional background material in these areas (see *Related Documentation* on next page).

Continued on next page

Preface, continued

SET documentation

The SET specification is documented in three volumes:

Book	Title	Contents
1	Business Description	Contains background information and processing flows for SET. Intended as a primer on software that both interfaces with payment systems and uses public-key cryptography.
2	Programmer’s Guide	Contains the technical specifications for the SET protocol. Primarily intended for use by software vendors who intend to create cardholder and merchant software.
3	Formal Protocol Definition	Contains the formal protocol definition for SET. Primarily intended for use by: • cryptographers analyzing security, • writers producing programming guides, and • system programmers developing cryptographic and messaging primitives.

Continued on next page

Preface, continued

Related documentation

The following articles and books contain additional background material. Readers are encouraged to consult these references for more information.

Answers to Frequently Asked Questions about Today's Cryptography, Paul Fahn, RSA Laboratories, 1993. (http://www.rsa.com/rsalabs/faq/)

Applied Cryptography, Second Edition, Bruce Schneier, John Wiley & Sons, Inc., 1996.

"Asymmetric Encryption: Evolution and Enhancements," Don B. Johnson and Stephen M. Matyas, *CryptoBytes,* volume 2, number 1, Spring 1996

BSAFE 2.1™, RSA Data Security, Inc., 1994. (http://www.rsa.com/rsa/prodspec/bsafe/rsa_bsaf.htm)

Data Encryption Standard, Federal Information Processing Standards Publication 46, 1977.

"The HMAC Construction," Mihir Bellare, Ran Canetti, and Hugo Krawczyk, *CryptoBytes,* volume 2, number 1, Spring 1996

HTML Sourcebook, Ian S. Graham, John Wiley & Sons, Inc., 1995.

The Internet for Everyone: A Guide for Users and Providers, Richard W. Wiggins, McGraw-Hill, Inc., 1995.

Optimal Asymmetric Encryption, M. Bellare and P. Rogaway, Eurocrypt 94. (http://www-cse.ucsd.edu/users/mihir/papers/oae.ps.gz)

An Overview of the PKCS Standards, Burton S. Kaliski, Jr., RSA Laboratories, 1993. (http://www.rsa.com/pub/pkcs/doc/ or http://www.rsa.com/pub/pkcs/ps/)

Public-Key Cryptography Standards (PKCS), RSA Data Security, Inc., Version 1.5, revised Nov. 1, 1993.

Extensions and Revisions to PKCS #7, RSA Data Security, Inc., May 13, 1997.

ITU Rec. X.509 (1993) | ISO/IEC 9594-8: 1995, including Draft Amendment 1: Certificate Extensions (Version 3 certificate).

RFC 1750, Randomness Recommendations for Security, D. Eastlake, S. Crocker, J. Schiller, December 1994.

Table of Contents

Preface i

1 Introduction 1
1.1 Background....................1
1.2 Objectives 4

2 Business Requirements....................6
2.1 Requirements 6
2.2 Features....................7
2.3 Scope 10

3 Concepts 12
3.1 Payment System Participants....................12
3.2 Cryptography 14
3.3 Certificate Issuance....................25
3.4 Kinds of Shopping 29

4 Payment Processing....................30
4.1 Overview 30
4.2 Cardholder Registration....................36
4.3 Merchant Registration....................47
4.4 Purchase Request 55
4.5 Payment Authorization 63
4.6 Payment Capture....................68

Table of Figures

FIGURE 1: SECRET-KEY CRYPTOGRAPHY 14
FIGURE 2: PUBLIC-KEY CRYPTOGRAPHY 15
FIGURE 3: ENCRYPTION OVERVIEW 20
FIGURE 4: HIERARCHY OF TRUST 27
FIGURE 5: GUIDE TO DIAGRAMS 32
FIGURE 6: CARDHOLDER REGISTRATION 36
FIGURE 7: MERCHANT REGISTRATION 47
FIGURE 8: PURCHASE REQUEST 55
FIGURE 9: PAYMENT AUTHORIZATION 63
FIGURE 10: PAYMENT CAPTURE 68

1 Introduction

1.1 Background

Impact of electronic commerce

There is no question that electronic commerce, as exemplified by the popularity of the Internet, is going to have an enormous impact on the financial services industry. No financial institution will be left unaffected by the explosion of electronic commerce.

- The number of payment card purchases made through this medium will grow as Internet-based online ordering systems are created.
- Many banks are planning to support this new form of electronic commerce by offering card authorizations directly over the Internet.
- Several trials with electronic currency and digital cash are already under way.

Projected use

With more than 30 million users today, and 90 million projected to come on board in the next two years, the Internet is a new way for businesses to establish computer-based resources that can be accessed by consumers as well as business partners around the world.

Internet

The Internet is changing the way we access and purchase information, communicate and pay for services, and acquire and pay for goods. Financial services such as bill payment, brokerage, insurance, and home banking are now or soon will be available over the Net. Any organization can become a global publisher by establishing an information site on the Internet’s World Wide Web.

World Wide Web

The Web - or other interactive transport mechanism - can display text, sound, images, and even video, allowing merchants to transmit information directly to potential consumers around the world and around the clock.

Consumer payment devices

With open networks, payments will be made increasingly by consumer-driven devices. As advanced technologies become more practical and affordable, the marketplace will move from “brick and mortar” to more convenient locations such as the home or office. As financial services evolve, consumers will consolidate their payment needs into one multi-functional relationship product that enables widespread, around-the-clock access.

Continued on next page

1.1 Background, continued

Publicity

Recently, an explosion of publicity has heralded the growth of the Internet and the possibilities for consumers and merchants to create a new type of shopping called *electronic commerce*. The publicity has focused on three areas:

- Marketing opportunities to develop new ways to browse, select, and pay for goods and services to on-line consumers,
- New products and services, and
- Security risks associated with sending unprotected financial information across public networks.

All three areas must be addressed to facilitate the future growth of payment card transaction volume in the electronic marketplace.

Role of payment systems

Payment systems and their financial institutions will play a significant role by establishing open specifications for payment card transactions that:

- provide for confidential transmission,
- authenticate the parties involved,
- ensure the integrity of payment instructions for goods and services order data , and
- authenticate the identity of the cardholder and the merchant to each other.

Procedures needed

Because of the anonymous nature of communications networks, procedures must be developed to substitute for existing procedures used in face-to-face or mail order/telephone order (MOTO) transactions including the authentication of the cardholder by the merchant. There is also a need for the cardholder to authenticate that the merchant accepts SET transactions and is authorized to accept payment cards.

Use of payment card products

Financial institutions have a strong interest in accelerating the growth of electronic commerce. Although electronic shopping and ordering do not require electronic payment, a much higher percentage of these transactions use payment card products instead of cash or checks. This will hold true in both the consumer marketplace and the commercial marketplace.

Continued on next page

1.1 Background, continued

Purpose of Secure Electronic Transaction

To meet these needs, the SET Secure Electronic Transaction protocol uses cryptography to:

- provide confidentiality of information,
- ensure payment integrity, and
- authenticate both merchants and cardholders.

This specification will enable greater payment card acceptance, with a level of security that will encourage consumers and businesses to make wide usage of payment card products in this emerging market.

1.2 Objectives

Motivation

Primary motivations for the payment card brands to provide specifications for secure payments are to:

- encourage the payment card community to take a leadership position in establishing a secure payment specification and, in so doing, to avoid costs associated with future reconciliation of implemented approaches,
- respect and preserve the relationship between merchants and Acquirers and between cardholders and Issuers,
- facilitate rapid development of the marketplace,
- respond quickly to the needs of the financial services market, and
- protect the integrity of payment card brands.

Payment security

The objectives of payment security are to:

- authenticate cardholders, merchants, and acquirers,
- provide confidentiality of payment data,
- preserve the integrity of payment data, and
- define the algorithms and protocols necessary for these security services.

Interoperability

The objectives of interoperability are to:

- clearly define detailed information to ensure that applications developed by various vendors will interoperate,
- create and support an open payment card standard,
- define exportable technology throughout, to encourage globally interoperable software,
- build on existing standards where practical,
- ensure compatibility with and acceptance by appropriate standards bodies, and
- allow for implementation on any combination of hardware and software platforms, such as PowerPC, Intel, Sparc, UNIX, MS-DOS, OS/2, Windows, and Macintosh.

Continued on next page

1.2 Objectives, continued

Market acceptance

The objectives of market acceptance are to:

- achieve global acceptance via ease of implementation and minimal impact on merchant and cardholder end users,
- allow for “bolt-on” implementation of the payment protocol to existing client applications,
- minimize change to the relationship between acquirers and merchants, and cardholders and issuers,
- allow for minimal impact to existing merchant, acquirer, and payment system applications and infrastructure, and
- provide a protocol that will be efficient for financial institutions.

2 Business Requirements

2.1 Requirements

Introduction

This section introduces the business requirements for secure payment processing using payment card products over both public networks (such as the Internet) and private networks.

Security issues non-competitive

Security issues regarding electronic commerce must be viewed as non-competitive in the interests of financial institutions, merchants, and cardholders.

Seven business requirements

SET addresses seven major business requirements:

1. Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
2. Ensure the integrity of all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded payment card account.
4. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.
5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties in an electronic commerce transaction.
6. Create a protocol that neither depends on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability among software and network providers.

2.2 Features

Features of the specification

These requirements are addressed by the following features of this specification:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication
- Interoperability

For the sake of clarity, each of these features is described as a distinct component. However, these elements do not function independently; all security functions must be implemented.

Confidentiality of information

To facilitate and encourage electronic commerce using payment card products, it will be necessary to assure cardholders that their payment information is safe and can only be accessed by the intended recipient. Therefore, cardholder account and payment information must be secured as it travels across the network, preventing interception of account numbers and expiration dates by unauthorized individuals.

Online shopping: In today’s on-line shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open networks with few security precautions, if any. However, this account information provides the key elements needed to create counterfeit cards and/or fraudulent transactions.

Fraud: While it is possible to obtain account information in other environments, there is a heightened concern about the ease of doing so with public network transactions. This concern reflects the potential for high-volume fraud, automated fraud (such as using filters on all messages passing over a network to extract all payment card account numbers from a data stream), and the potential for “mischievous fraud” that appears to be characteristic of some hackers.

In addition, the transmission of account information in a relatively unsecured manner has triggered a great deal of negative press.

SET’s use of message encryption ensures confidentiality of information (see Section 3.2).

Continued on next page

2.2 Features, continued

Integrity of data

The specification must guarantee that message content is not altered during the transmission between the originator and the recipient.

Payment information sent from cardholders to merchants includes order information, personal data, and payment instructions. If any component is altered in transit, the transaction will not be processed accurately. To eliminate this potential source of fraud and/or error, SET must provide the means to ensure that the contents of each order and payment message received matches the contents of the message sent.

SET provides for digital signatures, which ensure the integrity of payment information (see Section 3.2)

Cardholder account authentication

Merchants need a way to verify that a cardholder is a legitimate user of a valid branded payment card account number. A mechanism that uses technology to link a cardholder to a specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing.

This specification defines the mechanism to verify that a cardholder is a legitimate user of a valid payment card account number.

Note: This specification does not define the process used by a financial institution to determine whether an individual is a legitimate user of an account.

SET uses digital signatures and cardholder certificates to ensure the authentication of the cardholder account.

Continued on next page

2.2 Features, continued

Merchant authentication

The specification must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce.

SET provides for the use of digital signatures and merchant certificates to ensure authentication of the merchant (see Section 3.2).

Interoperability

The specification must be applicable on a variety of hardware and software platforms, and must not include a preference for one over another. Any cardholder with compliant software must be able to communicate with any merchant software that also meets the defined standard.

SET interoperability uses specific protocols and message formats to provide interoperability.

2.3 Scope

Use of payment cards

The SET specification addresses a portion of the message protocols that are necessary for electronic commerce. It specifically addresses those parts of the protocols that use or impact the use of payment cards.

Electronic shopping experience

The electronic shopping experience can be divided into several distinct stages.

Stage	Description
1	The cardholder browses for items in a variety of ways, such as: • using a browser to view an online catalog on the merchant's World Wide Web page; • viewing a catalog supplied by the merchant on a CD-ROM; or • looking at a paper catalog.
2	The cardholder selects items to be purchased.
3	The cardholder is presented with an order form containing the list of items, their prices, and a total price including shipping, handling, and taxes. This order form may be delivered electronically from the merchant's server or created on the cardholder's computer by electronic shopping software. Some online merchants may also support the ability for a cardholder to negotiate for the price of items (such as by presenting frequent shopper identification or information about a competitor's pricing).
4	The cardholder selects the means of payment. This specification focuses on the case when a payment card is selected.
5	The cardholder sends the merchant a completed order along with payment instructions. In this specification, the order and the payment instructions are digitally signed by cardholders who possess certificates.
6	The merchant requests payment authorization from the cardholder's financial institution.
7	The merchant sends confirmation of the order.

Continued on next page

2.3 Scope, continued

Electronic shopping experience (continued)

Stage	Description
8	The merchant ships the goods or performs the requested services from the order.
9	The merchant requests payment from the cardholder’s financial institution.

Although these stages are listed in a specific order, variations are possible; many such variations are described later in this specification.

This specification focuses on stages 5, 6, 7, and 9 when the cardholder chooses to use a payment card as the means of payment.

Within the scope

The following are within the scope of this specification:

- Application of cryptographic algorithms (such as RSA and DES)
- Certificate message and object formats
- Purchase messages and object formats
- Authorization messages and object formats
- Capture messages and object formats
- Message protocols between participants

Outside the scope

The following are outside the scope of this specification:

- Message protocols for offers, shopping, delivery of goods, etc.
- Operational issues such as the criteria set by individual financial institutions for the issuance of cardholder and merchant certificates
- Screen formats including the content, presentation and layout of order entry forms as defined by each merchant
- General payments beyond the domain of payment cards
- Security of data on cardholder, merchant, and payment gateway systems including protection from viruses, trojan horse programs, and hackers

Note: This is only a partial list of categories of things that are outside the scope of the SET specification.

3 Concepts

3.1 Payment System Participants

Interaction of participants

SET changes the way that participants in a payment system interact. In a face-to-face retail transaction or a mail order transaction, electronic processing begins with the merchant or the Acquirer. However, in a SET transaction, the electronic processing begins with the cardholder.

Cardholder

In the electronic commerce environment, consumers and corporate purchasers interact with merchants from personal computers. A cardholder uses a payment card that has been issued by an Issuer. SET ensures that in the cardholder’s interactions with the merchant, the payment card account information remains confidential.

Issuer

An Issuer is a financial institution that establishes an account for a cardholder and issues the payment card. The Issuer guarantees payment for authorized transactions using the payment card in accordance with payment card brand regulations and local legislation.

Merchant

A merchant offers goods for sale or provides services in exchange for payment. With SET, the merchant can offer its cardholders secure electronic interactions. A merchant that accepts payment cards must have a relationship with an Acquirer.

Acquirer

An Acquirer is the financial institution that establishes an account with a merchant and processes payment card authorizations and payments.

Payment gateway

A payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages, including payment instructions from cardholders.

Continued on next page

3.1 Payment System Participants, continued

Brand

Financial institutions have founded payment card brands that protect and advertise the brand, establish and enforce rules for use and acceptance of their payment cards, and provide networks to interconnect the financial institutions.

Other brands are owned by financial services companies that advertise the brand, and establish and enforce rules for use and acceptance of their payment cards. These brands combine the roles of Issuer and Acquirer in interactions with cardholders and merchants.

Third parties

Issuers and Acquirers sometimes choose to assign the processing of payment card transactions to third-party processors. This document does not distinguish between the financial institution and the processor of the transactions.

3.2 Cryptography

Protection of sensitive information

Cryptography has been used for centuries to protect sensitive information as it is transmitted from one location to another. In a cryptographic system, a message is encrypted using a key. The resulting ciphertext is then transmitted to the recipient where it is decrypted using a key to produce the original message. There are two primary encryption methods in use today: secret-key cryptography and public-key cryptography. SET uses both methods in its encryption process.

Secret-key cryptography

Secret-key cryptography, also known as symmetric cryptography, uses the same key to encrypt and decrypt the message. Therefore, the sender and the recipient of a message must share a secret, namely the key. A well known secret-key cryptography algorithm is the Data Encryption Standard (DES), which is used by financial institutions to encrypt PINs (personal identification numbers).

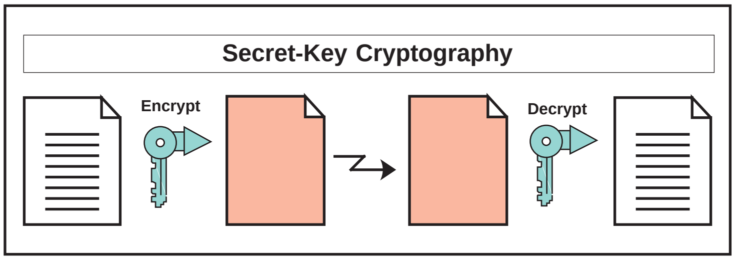


Figure 1: Secret-Key Cryptography

Continued on next page

3.2 Cryptography, continued

Public-key cryptography

Public-key cryptography, also known as asymmetric cryptography, uses two keys: one key to encrypt the message and the other key to decrypt the message. The two keys are mathematically related so that data encrypted with either key can only be decrypted using the other. Each user has two keys: a *public key* and a *private key*. The user distributes the public key. Because of the relationship between the two keys, the user and anyone receiving the public key can be assured that data encrypted with the public key and sent to the user can only be decrypted when the user uses the private key. *This assurance is only maintained if the user ensures that the private key is not disclosed to anyone else.* Therefore, the key pair should be generated by the user. The best known public-key cryptography algorithm is RSA (named after its inventors Rivest, Shamir, and Adleman).

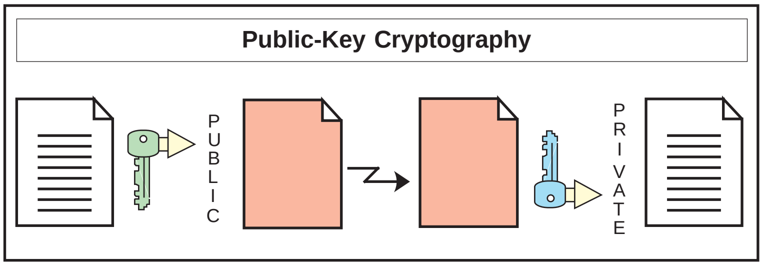


Figure 2: Public-Key Cryptography

Secret-key cryptography is impractical for exchanging messages with a large group of previously unknown correspondents over a public network. For a merchant to conduct transactions securely with millions of Internet subscribers, each consumer would need a distinct key assigned by that merchant and transmitted over a separate secure channel. On the other hand, by using public-key cryptography, that same merchant could create a public/private key pair and publish the public key, allowing any consumer to send a secure message to that merchant.

Continued on next page

3.2 Cryptography, continued

Encryption

Confidentiality is ensured by the use of message encryption.

Relationship of keys

When two users want to exchange messages securely, each of them transmits one component of their key pair, designated the public key, to the other and keeps secret the other component, designated the private key. Because messages encrypted with the public key can only be decrypted using the private key, these messages can be transmitted over an insecure network without fear that an eavesdropper could use the key to read encrypted transmissions.

For example, Bob can transmit a confidential message to Alice by encrypting the message using Alice's public key. As long as Alice ensures that no one else has access to her private key, both she and Bob will know that only Alice can read the message.

Use of symmetric key

SET will rely on cryptography to ensure message confidentiality. In SET, message data will be encrypted using a randomly generated symmetric encryption key. This key, in turn, will be encrypted using the message recipient's public key. This is referred to as the "digital envelope" of the message and is sent to the recipient along with the encrypted message itself. After receiving the digital envelope, the recipient decrypts it using his or her private key to obtain the randomly generated symmetric key and then uses the symmetric key to unlock the original message.

Note

To provide the highest degree of protection, it is essential that the programming methods and random number generation algorithms generate keys in a way that ensures that the keys cannot be easily reproduced using information about either the algorithms or the environment in which the keys are generated.

Continued on next page

3.2 Cryptography, continued

Digital signatures

Integrity and authentication are ensured by the use of digital signatures.

Relationship of keys

Because of the mathematical relationship between the public and private keys, data encrypted with either key can only be decrypted with the other. This allows the sender of a message to encrypt it using the sender's private key. Any recipient can determine that the message came from the sender by decrypting the message using the sender's public key.

For example, Alice can encrypt a known piece of data, such as her telephone number, with her private key and transmit it to Bob. When Bob decrypts the message using Alice's public key and compares the result to the known data, he can be sure that that the message could only have been encrypted using Alice's private key.

Using message digests

When combined with *message digests*, encryption using the private key allows users to digitally sign messages. A message digest is a value generated for a message (or document) that is unique to that message.[1] A message digest is generated by passing the message through a one-way cryptographic function; that is, one that cannot be reversed. When the digest of a message is encrypted using the sender's private key and is appended to the original message, the result is known as the digital signature of the message.

The recipient of the digital signature can be sure that the message really came from the sender. And, because changing even one character in the message changes the message digest in an unpredictable way, the recipient can be sure that the message was not changed after the message digest was generated.

Continued on next page

[1] The algorithm used by SET generates 160-bit message digests. The algorithm is such that changing a single bit in the message will change, on average, half of the bits in the message digest. Roughly, the odds of two messages having the same message digest are one in 1,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000. It is computationally unfeasible to generate two different messages that have the same message digest.

3.2 Cryptography, continued

Example of the use of a digital signature

For example, Alice computes the message digest of a property description and encrypts it with her private key yielding a digital signature for the message. She transmits both the message and the digital signature to Bob. When Bob receives the message, he computes the message digest of the property description and decrypts the digital signature with Alice's public key. If the two values match, Bob knows that the message was signed using Alice's private key and that it has not changed since it was signed.

Two key pairs

SET uses a distinct public/private key pair to create the digital signature. Thus, each SET participant will possess two asymmetric key pairs: a "key exchange" pair, which is used in the process of encryption and decryption, and a "signature" pair for the creation and verification of digital signatures. Note that the roles of the public and private keys are reversed in the digital signature process where the private key is used to encrypt (sign) and the public key is used to decrypt (verify the signature).

Continued on next page

3.2 Cryptography, continued

Certificates

Authentication is further strengthened by the use of certificates.

Need for authentication

Before two parties use public-key cryptography to conduct business, each wants to be sure that the other party is authenticated. Before Bob accepts a message with Alice's digital signature, he wants to be sure that the public key belongs to Alice and not to someone masquerading as Alice on an open network. One way to be sure that the public key belongs to Alice is to receive it over a secure channel directly from Alice. However, in most circumstances this solution is not practical.

Need for a trusted third party

An alternative to secure transmission of the key is to use a trusted third party to authenticate that the public key belongs to Alice. Such a party is known as a *Certificate Authority* (CA). The Certificate Authority authenticates Alice's claims according to its published policies. For example, a Certificate Authority could supply certificates that offer a high assurance of personal identity, which may be required for conducting business transactions; this Certificate Authority may require Alice to present a driver's license or passport to a notary public before it will issue a certificate. Once Alice has provided proof of her identity, the Certificate Authority creates a message containing Alice's name and her public key. This message, known as a *certificate*, is digitally signed by the Certificate Authority. It contains owner identification information, as well as a copy of one of the owner's public keys ("key exchange" or "signature"). To get the most benefit, the public key of the Certificate Authority should be known to as many people as possible. Thus, by trusting a single key, an entire hierarchy can be established in which one can have a high degree of trust.

Because SET participants have two key pairs, they also have two certificates. Both certificates are created and signed at the same time by the Certificate Authority.

SET authentication

The means that a financial institution uses to authenticate a cardholder or merchant is not defined by this specification. Each payment card brand and financial institution will select an appropriate method.

Continued on next page

3.2 Cryptography, continued

Encryption summary

This diagram provides an overview of the entire encryption process when Alice wishes to sign, for example, a property description and send it in an encrypted message to Bob. The numbered steps in the diagram are explained on the following pages.

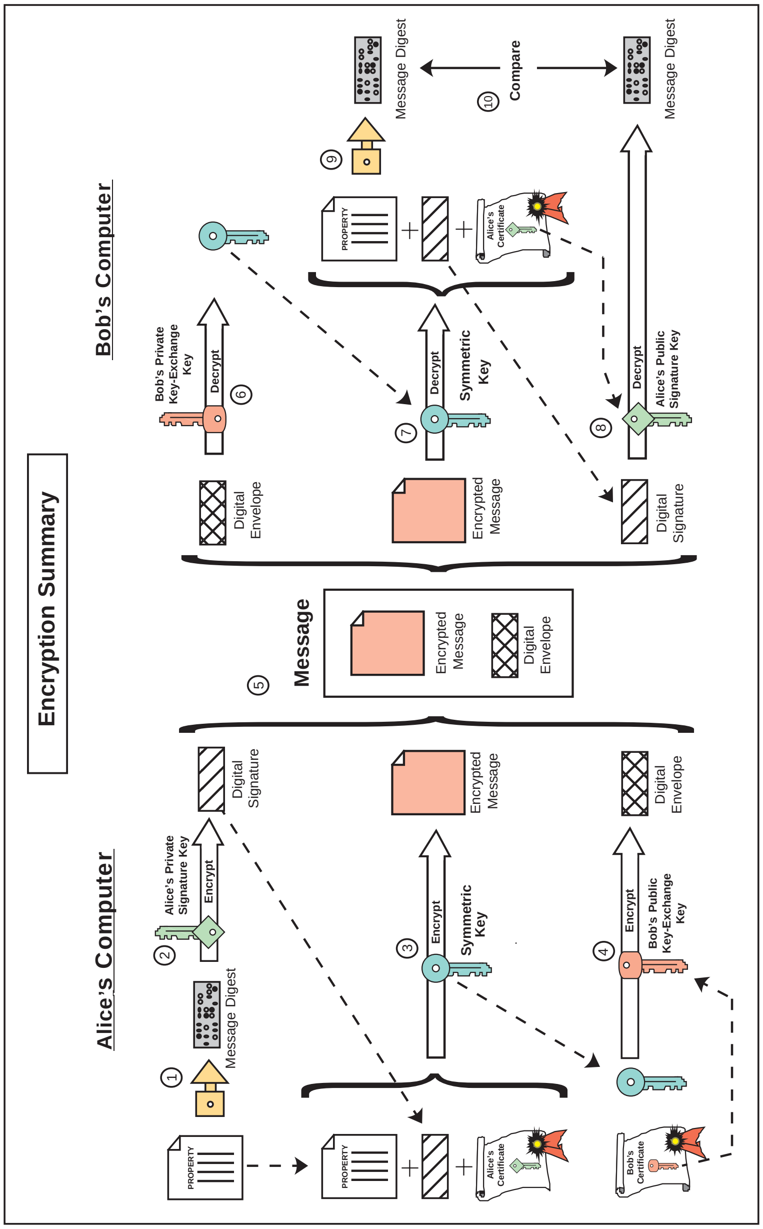


Figure 3: Encryption Overview

Continued on next page

3.2 Cryptography, continued

Encryption

The encryption process in Figure 3 consists of the following steps:

Step	Description
1	Alice runs the property description through a one-way algorithm to produce a unique value known as the message digest. This is a kind of digital fingerprint of the property description and will be used later to test the integrity of the message.
2	She then encrypts the message digest with her private signature key to produce the digital signature.
3	Next, she generates a random symmetric key and uses it to encrypt the property description, her signature and a copy of her certificate, which contains her public signature key. To decrypt the property description, Bob will require a secure copy of this random symmetric key.
4	Bob’s certificate, which Alice must have obtained prior to initiating secure communication with him, contains a copy of his public key-exchange key. To ensure secure transmission of the symmetric key, Alice encrypts it using Bob’s public key-exchange key. The encrypted key, referred to as the digital envelope, will be sent to Bob along with the encrypted message itself.
5	Alice sends a message to Bob consisting of the following: the symmetrically encrypted property description, signature and certificate, as well as the asymmetrically encrypted symmetric key (the digital envelope).

Continued on next page

3.2 Cryptography, continued

Decryption

Likewise, the decryption process consists of the following steps:

Step	Description
6	Bob receives the message from Alice and decrypts the digital envelope with his private key-exchange key to retrieve the symmetric key.
7	He uses the symmetric key to decrypt the property description, Alice's signature, and her certificate.
8	He decrypts Alice's digital signature with her public signature key, which he acquires from her certificate. This recovers the original message digest of the property description.
9	He runs the property description through the same one-way algorithm used by Alice and produces a new message digest of the decrypted property description.
10	Finally, he compares his message digest to the one obtained from Alice's digital signature. If they are exactly the same, he confirms that the message content has not been altered during transmission and that it was signed using Alice's private signature key. If they are not the same, then the message either originated somewhere else or was altered after it was signed. In that case, Bob takes some appropriate action such as notifying Alice or discarding the message.

Continued on next page

3.2 Cryptography, continued

Dual signature

SET introduces a new application of digital signatures, namely the concept of dual signatures. To understand the need for this new concept, consider the following scenario: Bob wants to send Alice an offer to purchase a piece of property and an authorization to his bank to transfer the money if Alice accepts the offer, but Bob doesn't want the bank to see the terms of the offer nor does he want Alice to see his account information. Further, Bob wants to link the offer to the transfer so that the money is only transferred if Alice accepts his offer. He accomplishes all of this by digitally signing both messages with a single signature operation that creates a dual signature.

Generating a dual signature

A dual signature is generated by creating the message digest of both messages, concatenating the two digests together, computing the message digest of the result and encrypting this digest with the signer's private signature key. The signer must include the message digest of the other message in order for the recipient to verify the dual signature. A recipient of either message can check its authenticity by generating the message digest on its copy of the message, concatenating it with the message digest of the other message (as provided by the sender) and computing the message digest of the result. If the newly generated digest matches the decrypted dual signature, the recipient can trust the authenticity of the message.

Example

If Alice accepts Bob's offer, she can send a message to the bank indicating her acceptance and including the message digest of the offer. The bank can verify the authenticity of Bob's transfer authorization and ensure that the acceptance is for the same offer by using its digest of the authorization and the message digest presented by Alice of the offer to validate the dual signature. Thus the bank can check the authenticity of the offer against the dual signature, but the bank cannot see the terms of the offer.

Use of dual signatures

Within SET, dual signatures are used to link an order message sent to the merchant with the payment instructions containing account information sent to the Acquirer. When the merchant sends an authorization request to the Acquirer, it includes the payment instructions sent to it by the cardholder and the message digest of the order information. The Acquirer uses the message digest from the merchant and computes the message digest of the payment instructions to check the dual signature.

Continued on next page

3.2 Cryptography, continued

Import/export issues

A number of governments have regulations regarding the import or export of cryptography. As a general rule, these governments allow cryptography to be used when:

- the data being encrypted is of a financial nature;
- the content of the data is well-defined;
- the length of the data is limited; and
- the cryptography cannot easily be used for other purposes.

The SET protocol is limited to the financial portion of shopping and the content of the SET messages has been carefully reviewed to satisfy the concerns of governments. As long as software vendors can demonstrate that the cryptography used for SET cannot easily be put to other purposes, import and export licenses should be obtainable.

3.3 Certificate Issuance

Cardholder certificates

Cardholder certificates function as an electronic representation of the payment card. Because they are digitally signed by a financial institution, they cannot be altered by a third party and and can only be generated by a financial institution. A cardholder certificate does not contain the account number and expiration date. Instead the account information and a secret value known only to the cardholder's software are encoded using a one-way hashing algorithm. If the account number, expiration date, and the secret value are known, the link to the certificate can be proven, but the information cannot be derived by looking at the certificate. Within the SET protocol, the cardholder supplies the account information and the secret value to the payment gateway where the link is verified.

A certificate is only issued to the cardholder when the cardholder's issuing financial institution approves it. By requesting a certificate, a cardholder has indicated the intent to perform commerce via electronic means. This certificate is transmitted to merchants with purchase requests and encrypted payment instructions. Upon receipt of the cardholder's certificate, a merchant can be assured, at a minimum, that the account number has been validated by the card-issuing financial institution or its agent.

In this specification, cardholder certificates are optional at the payment card brand's discretion.

Merchant certificates

Merchant certificates function as an electronic substitute for the payment brand decal that appears in the store window—the decal itself is a representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand. Because they are digitally signed by the merchant's financial institution, merchant certificates cannot be altered by a third party and can only be generated by a financial institution.

These certificates are approved by the acquiring financial institution and provide assurance that the merchant holds a valid agreement with an Acquirer. A merchant must have at least one pair of certificates to participate in the SET environment, but there may be multiple certificate pairs per merchant. A merchant will have a pair of certificates for each payment card brand that it accepts.

Continued on next page

3.3 Certificate Issuance, continued

Payment gateway certificates

Payment gateway certificates are obtained by Acquirers or their processors for the systems that process authorization and capture messages. The gateway's encryption key, which the cardholder gets from this certificate, is used to protect the cardholder's account information.

Payment gateway certificates are issued to the Acquirer by the payment brand.

Acquirer certificates

An Acquirer must have certificates in order to operate a Certificate Authority that can accept and process certificate requests directly from merchants over public and private networks. Those Acquirers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Acquirers receive their certificates from the payment card brand.

Issuer certificates

An Issuer must have certificates in order to operate a Certificate Authority that can accept and process certificate requests directly from cardholders over public and private networks. Those Issuers that choose to have the payment card brand process certificate requests on their behalf will not require certificates because they are not processing SET messages. Issuers receive their certificates from the payment card brand.

Continued on next page

3.3 Certificate Issuance, continued

Hierarchy of trust

SET certificates are verified through a hierarchy of trust. Each certificate is linked to the signature certificate of the entity that digitally signed it. By following the trust tree to a known trusted party, one can be assured that the certificate is valid. For example, a cardholder certificate is linked to the certificate of the Issuer (or the Brand on behalf of the Issuer). The Issuer's certificate is linked back to a root key through the Brand's certificate. The public signature key of the root is known to all SET software and may be used to verify each of the certificates in turn. The following diagram illustrates the hierarchy of trust.

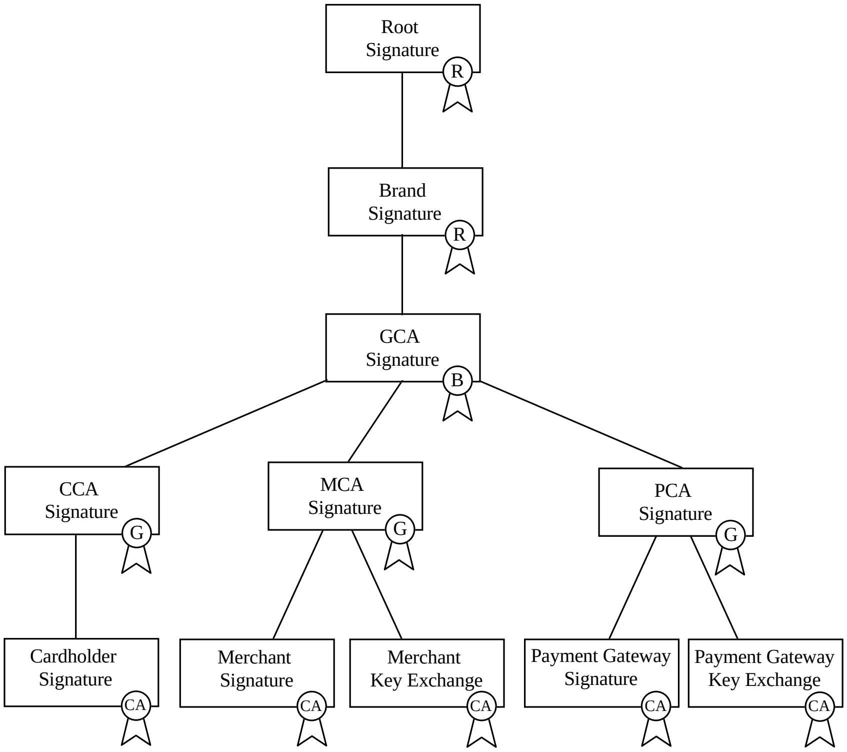


Figure 4: Hierarchy of Trust

The number of levels shown in this diagram is illustrative. A payment card brand may not always operate a geopolitical Certificate Authority between itself and the financial institutions.

Continued on next page

3.3 Certificate Issuance, continued

Root key distribution

The root key will be distributed in a self-signed certificate. This root key certificate will be available to software vendors to include with their software.

Root key validation

Software can confirm that it has a valid root key by sending an initiate request to the Certificate Authority that contains the hash of the root certificate. In the event that the software does not have a valid root certificate, the Certificate Authority will send one in the response.

Note: In this extremely unusual case where the software's root key is invalid, the user (cardholder or merchant) will have to enter a string that corresponds to the hash of the certificate. This confirmation hash must be obtained from a reliable source, such as the cardholder's financial institution.

Root key replacement

When the root key is generated, a replacement key is also generated. The replacement key is stored securely until it is needed.

The self-signed root certificate and the hash of the replacement key are distributed together.

Software will be notified of the replacement through a message that contains a self-signed certificate of the replacement root and the hash of the next replacement root key.

Software validates the replacement root key by calculating its hash and comparing it with the hash of the replacement key contained in the root certificate.

3.4 Kinds of Shopping

Variety of experiences

Cardholders will shop in many different ways, including the use of online catalogs and electronic catalogs. The SET protocol supports each of these shopping experiences and should support others as they are defined.

Online catalogs

The growth of electronic commerce is attributed largely to the popularity of the World Wide Web. Merchants can tap into this popularity by creating virtual storefronts on the Web that contain online catalogs. They can quickly update these catalogs as their product offerings change for seasonal promotions or other reasons.

A cardholder can visit these Web pages and select items to order. When the cardholder finishes shopping and submits a request, the merchant's Web server can send the cardholder a completed order form to review and approve.

Once the cardholder approves the order and designates a payment card, the SET protocol enables the cardholder to transmit payment instructions by a secure means, while enabling the merchant to obtain authorization and receive payment.

Electronic catalogs

A growing number of merchants are distributing their catalogs via electronic media such as diskette or CD-ROM. This approach allows the cardholder to browse through merchandise off-line. With an on-line catalogue, the merchant has to be concerned about bandwidth and may choose to include fewer graphics or reduce the resolution of the graphics. By providing an off-line catalogue, such constraints are significantly reduced.

In addition, the merchant may provide a custom shopping application tailored to the merchandise in the electronic catalogue. Cardholders will shop by browsing through the catalogue and selecting items to include on an order.

Once the cardholder approves the order and chooses to use a payment card, an electronic message using the SET protocol can be sent to the merchant with the order and payment instructions. This message can be delivered on-line, such as to the merchant's Web page, or sent via a store-and-forward mechanism, such as electronic mail.

4 Payment Processing

4.1 Overview

Purpose

This chapter describes the flow of transactions as they are processed by various systems.

Protocol description

In the event that the description of the processing in this book differs from that in Book 3: Formal Protocol Definition, the Formal Protocol Definition takes precedence.

Transactions described

SET defines a variety of transaction protocols that use the cryptographic concepts introduced in Chapter 3 to securely conduct electronic commerce. This chapter describes the following transactions:

Transaction	Topic
Cardholder registration	4.2
Merchant registration	4.3
Purchase request	4.4
Payment authorization	4.5
Payment capture	4.6

Continued on next page

4.1 Overview, continued

Other transactions

The additional transactions listed below are part of the SET specification, but are not described in this book. For more information about these transactions, see Book 2: Programmer's Guide.

Certificate inquiry and status	If the CA is unable to complete the processing of a certificate request quickly, it will send a reply to the cardholder or merchant indicating that the requester should check back later. The cardholder or merchant sends the *Certificate Inquiry* message to determine the status of the certificate request and to receive the certificate if the request has been approved.
Purchase inquiry	Allows the cardholder to check the status of the processing of an order after the purchase response has been received. Note that this message does not include information such as the status of back ordered goods, but does indicate the status of authorization, capture and credit processing.
Authorization reversal	Allows a merchant to correct previous authorization requests. If the order will not be completed, the merchant reverses the entire authorization. If part of the order will not be completed (such as when goods are back ordered), the merchant reverses part of the amount of the authorization.
Capture reversal	Allows a merchant to correct errors in capture requests such as transaction amounts that were entered incorrectly by a clerk.
Credit	Allows a merchant to issue a credit to a cardholder's account such as when goods are returned or were damaged during shipping. Note that the SET *Credit* message is always initiated by the merchant, not the cardholder. All communications between the cardholder and merchant that result in a credit being processed happen outside of SET.
Credit reversal	Allows a merchant to correct a previously request credit.
Payment gateway certificate request	Allows a merchant to query the Payment Gateway and receive a copy of the gateway's current key-exchange and signature certificates.
Batch administration	Allows a merchant to communicate information to the Payment Gateway regarding merchant batches.
Error message	Indicates that a responder rejects a message because it fails format or content verification tests.

Continued on next page

4.1 Overview, continued

Guide to the diagrams

The following abbreviations are use in the detailed diagrams in this chapter to indicate the participant who digitally signs a message or certificate.

Initial	Participant
C	Cardholder
M	Merchant
P	Payment Gateway
CA	Certificate Authority

The following symbols are used in the detailed diagrams:

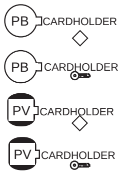
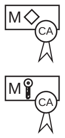
Symbol	Description
 PB CARDHOLDER PB CARDHOLDER PV CARDHOLDER PV CARDHOLDER	These are cryptographic keys. - The “teeth” of the key indicate the key’s owner. - Keys with “PB” on the handle are public keys, and those with “PV” are private keys. Private keys are always known to their owner. - Keys with a diamond (◇) are signature keys and those with a small key (🗝)are key-exchange keys.
	This is a digital signature. The initial indicates which private key was used to create the signature. For example, this signature was created by the merchant private signature key.
	This is a dual signature. The initial indicates which private key was used to create the signature. For example, this dual signature was created by the cardholder private signature key.
	These are certificates. - The initial in the “seal” indicates which private key was used to sign the certificate. - The letter on the certificate indicates the public key being certified. - The diamond and key symbols distinguish signature certificates from key-exchange certificates. The “CA” in these symbols indicates that these certificates were created by the Certificate Authority, and the “M” indicates they are merchant certificates.

Figure 5: Guide to Diagrams

Continued on next page

4.1 Overview, continued

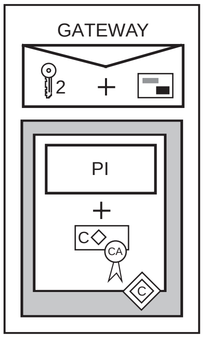
🔑1	This is a symmetric key used to encrypt data. It will always be sent with the encrypted data in the digital envelope. The number following the key differentiates symmetric keys used in a transaction set.
💳	This is a payment card and is used to indicate when the cardholder’s account number is being transmitted in the digital envelope along with the symmetric encryption key.
☰	This is protected data. It is used to represent account information sent in the digital envelope of registration requests for merchants and payment gateways.
	This is an encrypted message including the digital envelope. The data in the shaded region has been encrypted using a randomly generated symmetric key (identified here as the second such key generated for this transaction set). The entity whose public key was used to encrypt the envelope is identified above the envelope (in this case, the Payment Gateway). Note that in this case the digital envelope includes both the symmetric key and the cardholder’s account number. Also note that the portion of the message encrypted using the symmetric key contains the cardholder’s signature certificate and was dual signed by the cardholder.

Figure 5: Guide to Diagrams, continued

Note: **Bold text** in the detailed diagrams in sections 4.2 - 4.6 denotes that the particular step requires user participation. The reader should assume that all other steps are automated by SET software and require at most minimal user interaction (that is, either the software displays an acknowledgment message or the user must perform a trivial action like clicking an icon).

Continued on next page

4.1 Overview, continued

Certificate Authority functions

Sections 4.2 and 4.3 include diagrams that describe the processing flows of the Certificate Authority. The primary functions of the Certificate Authority are to:

- receive registration requests,
- process and approve/decline requests, and
- issue certificates.

The processing flows describe these functions as though they are performed by a single entity, but they actually may be performed by one to three entities. Payment card brands and individual financial institutions will review their business needs for these functions to select a solution for implementation. The selected solution may be to implement a single-server device that provides the Certificate Authority functions or multiple devices that distribute the processing.

The following list suggests some *possible* arrangements with variations on distribution:

- A company that issues proprietary cards may perform all three steps for its cardholders.
- A financial institution may receive, process, and approve certificate requests for its cardholders or merchants, and forward the information to the appropriate payment card brand(s) to issue the certificates.
- An independent *Registration Authority* that processes payment card certificate applications for multiple payment card brands may receive certificate requests and forward them to the appropriate financial institution (Issuer or Acquirer) for processing; the financial institution forwards approved requests to the payment card brands to issue the certificates.

These scenarios simply suggest some possible arrangements. Payment card brands and financial institutions will select an appropriate solution based on their individual business needs.

Continued on next page

4.1 Overview, continued

Optional cardholder certificates

The diagrams and processing flows that follow describe the processing of the transactions when the cardholder is in possession of a signature certificate issued under the trust hierarchy of the payment card brand. Payment card brands at their option may allow cardholders to process transactions without a certificate as a temporary measure to facilitate implementation of this specification.

Cardholder authentication

The SET protocol uses a cardholder signature certificate to confirm that a transaction is from a registered user of a payment card.

Strength of cardholder certificates

A cardholder certificate is not a guarantee of the identity of the cardholder. The strength of a cardholder certificate is wholly dependent on the methods used by the payment card brand and the payment card issuer to authenticate the cardholder prior to the certificate being issued.

No digital signature

When a cardholder does not possess a signature certificate, no digital signature is generated. In place of the digital signature, the cardholder generates the message digest of the data and inserts the message digest into the digital envelope.

Assurance of integrity

The recipient of data from the cardholder uses the message digest from the digital envelope to confirm the integrity of the data.

4.2 Cardholder Registration

Figure 6 provides a high-level overview of the cardholder registration process, showing its seven fundamental steps. The detailed sections that follow describe each step. The icon to the left corresponds to Figure 6 and serves as a map to the scenario; it is repeated in the more detailed sections with a shaded region that indicates which step is being described.

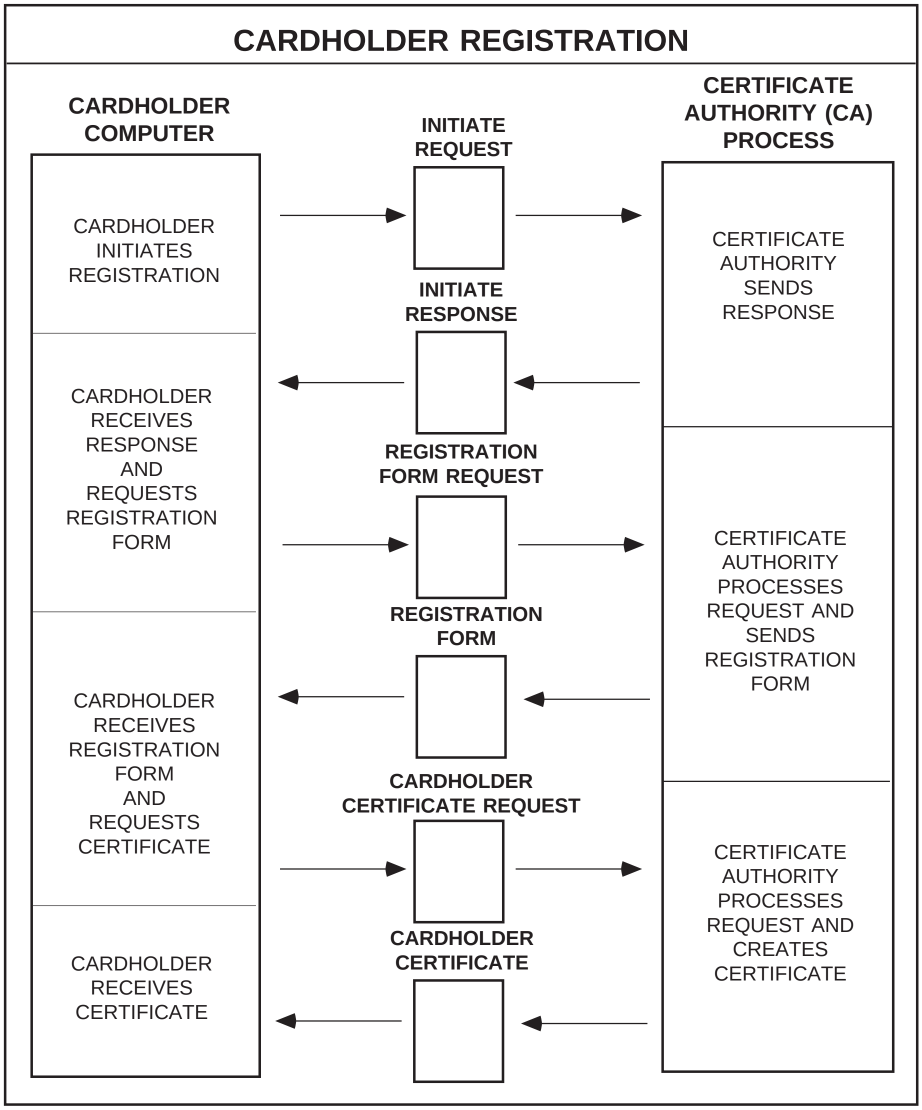

CARDHOLDER REGISTRATION
CARDHOLDER COMPUTER
CERTIFICATE AUTHORITY (CA) PROCESS
CARDHOLDER INITIATES REGISTRATION
INITIATE REQUEST
CERTIFICATE AUTHORITY SENDS RESPONSE
INITIATE RESPONSE
CARDHOLDER RECEIVES RESPONSE AND REQUESTS REGISTRATION FORM
REGISTRATION FORM REQUEST
CERTIFICATE AUTHORITY PROCESSES REQUEST AND SENDS REGISTRATION FORM
REGISTRATION FORM
CARDHOLDER RECEIVES REGISTRATION FORM AND REQUESTS CERTIFICATE
CARDHOLDER CERTIFICATE REQUEST
CERTIFICATE AUTHORITY PROCESSES REQUEST AND CREATES CERTIFICATE
CARDHOLDER CERTIFICATE
CARDHOLDER RECEIVES CERTIFICATE

Figure 6: Cardholder Registration

Continued on next page

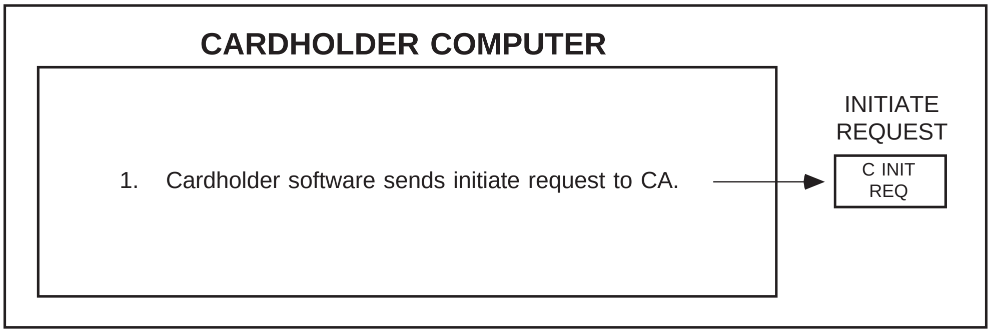
4.2 Cardholder Registration, continued

Cardholders must register with a Certificate Authority (CA) before they can send SET messages to merchants. In order to send SET messages to the CA, the cardholder must have a copy of the CA public key-exchange key, which is provided in the CA key-exchange certificate.

The cardholder also needs a copy of the registration form from the cardholder's financial institution. In order for the CA to provide the registration form, the cardholder software must identify the issuing financial institution to the CA. Obtaining the registration form requires two exchanges between the cardholder software and the CA.

The registration process is started when the cardholder software requests a copy of the CA's key-exchange certificate.

Cardholder initiates registration

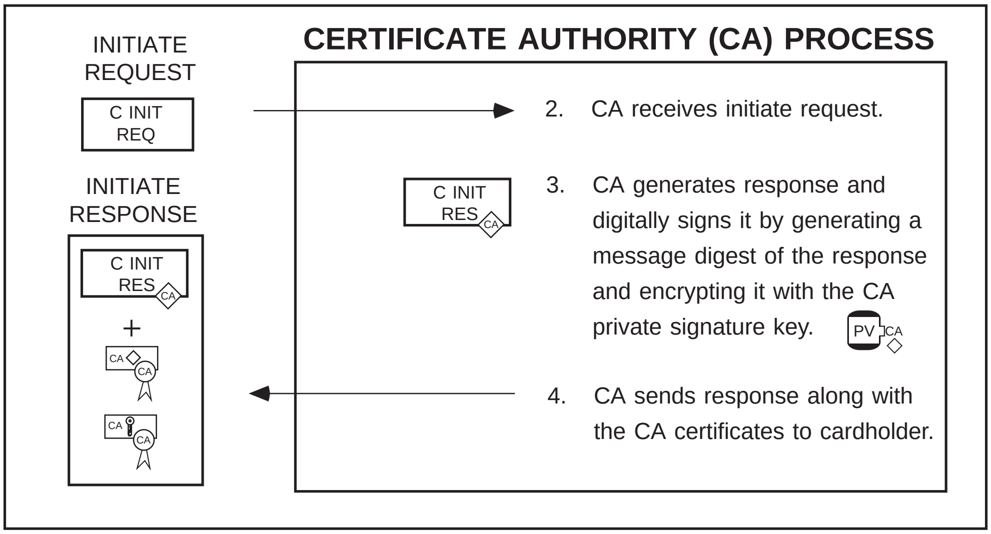


Continued on next page

4.2 Cardholder Registration, continued

When the CA receives the request, it transmits its certificates to the cardholder. The CA key-encryption certificate provides the cardholder software with the information necessary to protect the payment card account number in the registration form request.

Certificate Authority sends response



2. CA receives initiate request.

3. CA generates response and digitally signs it by generating a message digest of the response and encrypting it with the CA private signature key.

4. CA sends response along with the CA certificates to cardholder.

Continued on next page

4.2 Cardholder Registration, continued

The cardholder software verifies the CA certificate by traversing the trust chain to the root key, as described in Section 3.3. The software must hold the CA certificates to use later during the registration process. Once the software has a copy of the CA key-exchange certificate, the cardholder can request a registration form.

The cardholder software creates a registration form request message. Next the software generates a random symmetric encryption key. It uses this random key to encrypt the registration form request message. The random key is then encrypted along with the account number into the digital envelope using the CA public key-exchange key. Finally, the software transmits all of these components to the CA.

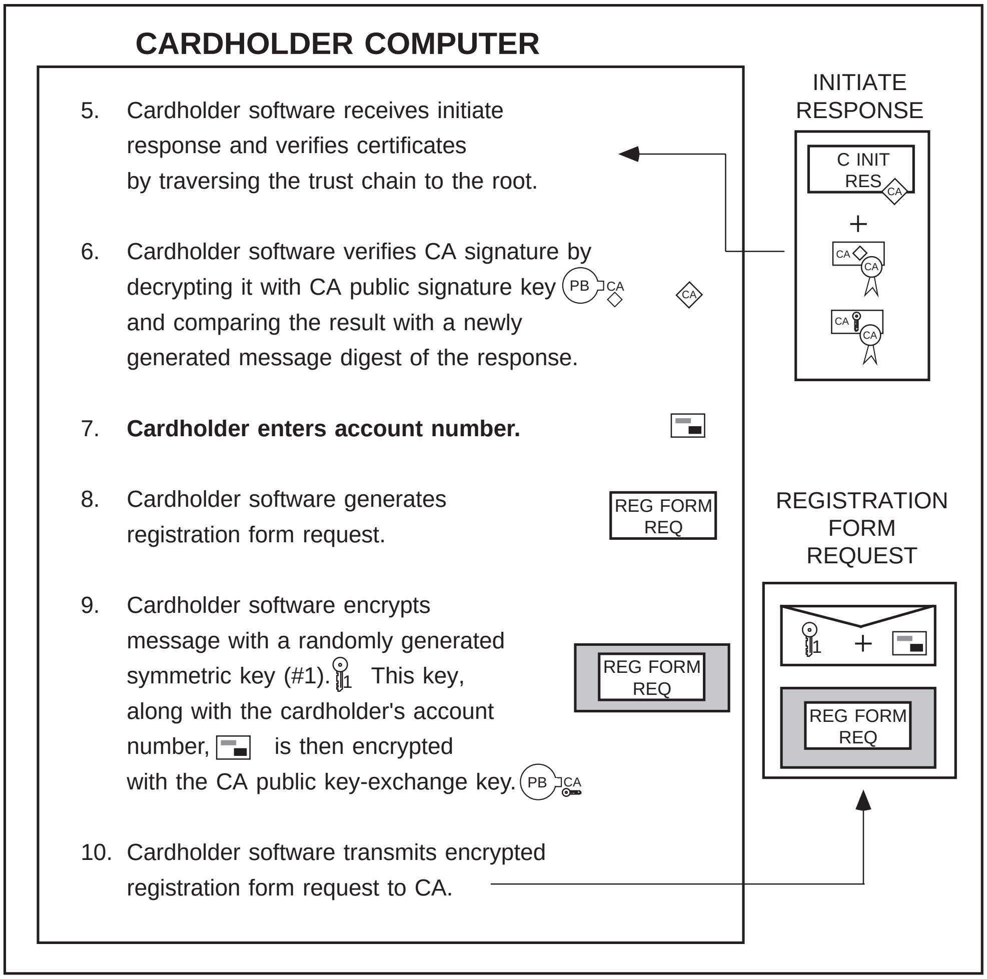
The cardholder software:

- verifies the CA certificate by traversing the trust chain to the root key,
- holds the CA certificates to use later during the registration process,
- creates a registration form request message,
- generates a random symmetric encryption key,
- uses this random key to encrypt the registration form request message,
- encrypts the random key along with the account number into the digital envelope using the CA public key-exchange key,
- transmits all of these components to the CA.

Continued on next page

4.2 Cardholder Registration, continued

Cardholder receives response and requests registration form



CARDHOLDER COMPUTER

5. Cardholder software receives initiate response and verifies certificates by traversing the trust chain to the root.

6. Cardholder software verifies CA signature by decrypting it with CA public signature key PB CA and comparing the result with a newly generated message digest of the response.

7. **Cardholder enters account number.**

8. Cardholder software generates registration form request.

9. Cardholder software encrypts message with a randomly generated symmetric key (#1). 1 This key, along with the cardholder's account number, ▨ is then encrypted with the CA public key-exchange key. PB CA

10. Cardholder software transmits encrypted registration form request to CA.

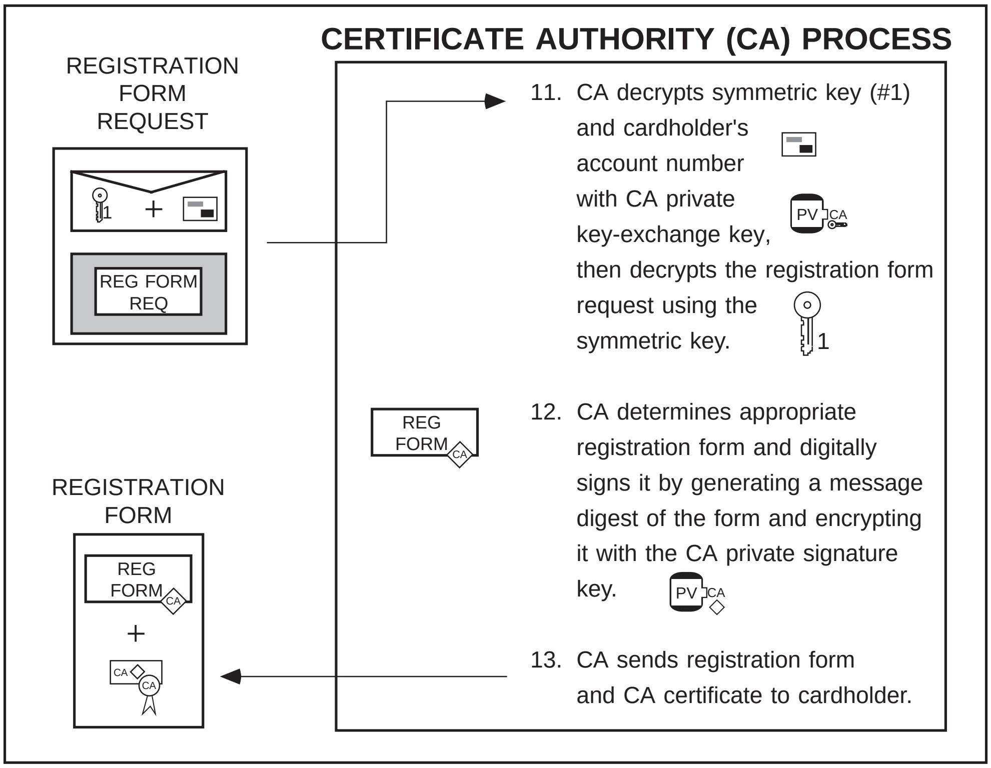
Continued on next page

4.2 Cardholder Registration, continued

The CA identifies the cardholder's financial institution (using the first six to eleven digits of the account number) and selects the appropriate registration form. It digitally signs and then returns this registration form to the cardholder.

In some cases, the CA may not have a copy of the registration form but can inform the cardholder software where the form can be obtained. For example, the cardholder's issuing financial institution may operate its own CA. In this event, the CA returns a referral response instead of the registration form. (This referral response is not shown in the diagram below.)

Certificate Authority processes request and sends registration form



11. CA decrypts symmetric key (#1) and cardholder's account number with CA private key-exchange key, then decrypts the registration form request using the symmetric key.

12. CA determines appropriate registration form and digitally signs it by generating a message digest of the form and encrypting it with the CA private signature key.

13. CA sends registration form and CA certificate to cardholder.

Continued on next page

4.2 Cardholder Registration, continued

The cardholder software verifies the CA certificate by traversing the trust chain to the root key.

The cardholder needs a signature public/private key pair for use with SET. The cardholder software generates this key pair if it does not already exist.

To register an account, the cardholder fills out the registration form that was returned by the CA with information such as the cardholder’s name, expiration date, account billing address, and any additional information the issuing financial institution deems necessary to identify the certificate requester as the valid cardholder.

The cardholder software generates a random number that will be used by the CA in generating the certificate. The usage of this random number is described in the processing performed by the CA.

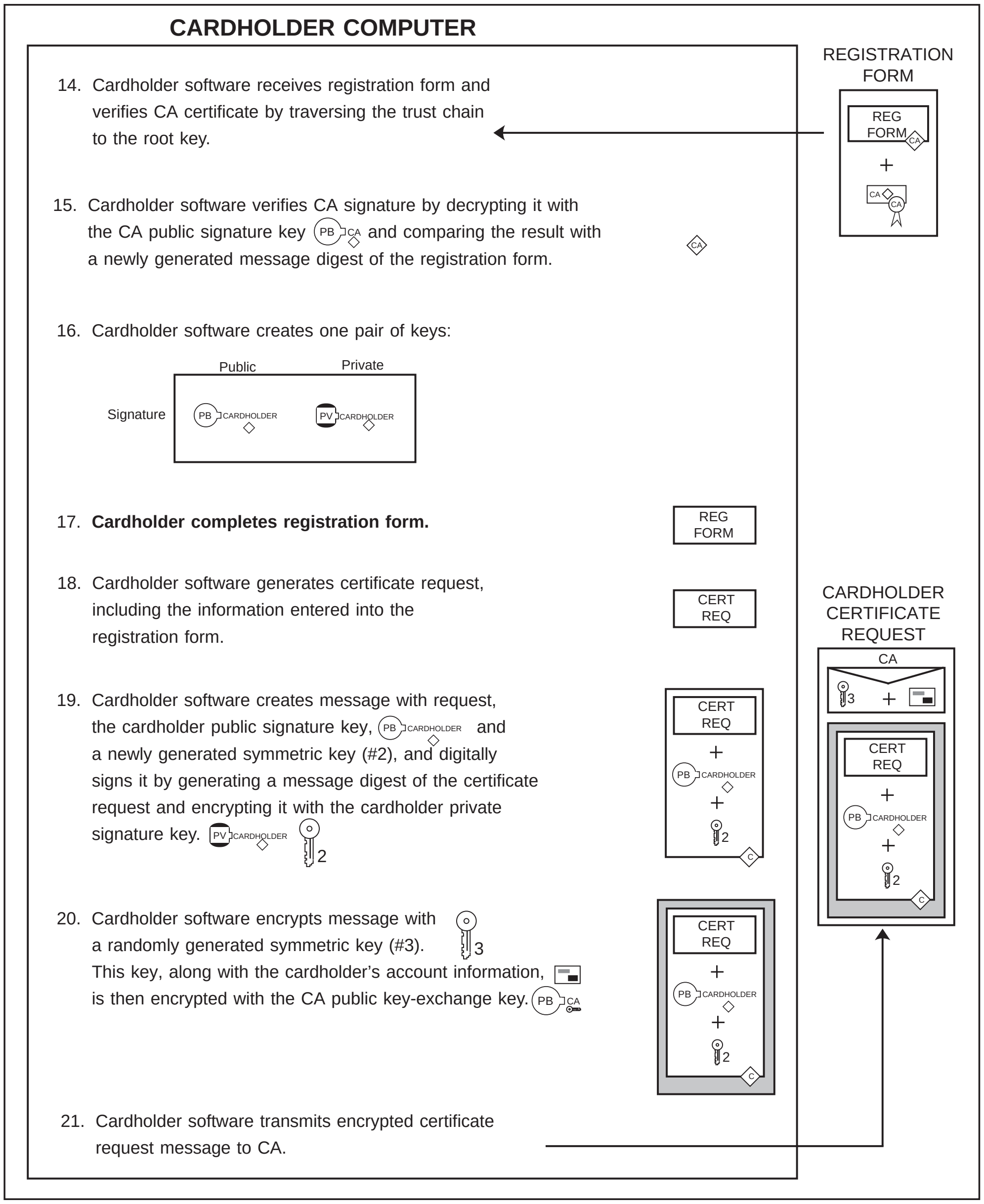
The cardholder software takes this registration information and combines it with the public key in a registration message. The software digitally signs the registration message. Next the software generates two random symmetric encryption keys. The software places one random key inside the message; the CA will use this key to encrypt the response. It uses the other random key to encrypt the registration message. This random key is then encrypted along with the account number, expiration date, and the random number into the digital envelope using the CA public key-exchange key. Finally, the software transmits all of these components to the CA.

Note: If the CA returned a referral response as described earlier in the CA processing, the cardholder software will return to the beginning of the registration process communicating with the referral CA to receive that CA’s certificates and the appropriate registration form.

Continued on next page

4.2 Cardholder Registration, continued

Cardholder receives registration form and requests certificate



14. Cardholder software receives registration form and verifies CA certificate by traversing the trust chain to the root key.

15. Cardholder software verifies CA signature by decrypting it with the CA public signature key PB CA and comparing the result with a newly generated message digest of the registration form.

16. Cardholder software creates one pair of keys:

17. **Cardholder completes registration form.**

18. Cardholder software generates certificate request, including the information entered into the registration form.

19. Cardholder software creates message with request, the cardholder public signature key, PB CARDHOLDER and a newly generated symmetric key (#2), and digitally signs it by generating a message digest of the certificate request and encrypting it with the cardholder private signature key. PV CARDHOLDER 2

20. Cardholder software encrypts message with a randomly generated symmetric key (#3). 3 This key, along with the cardholder's account information, is then encrypted with the CA public key-exchange key. PB CA

21. Cardholder software transmits encrypted certificate request message to CA.

Continued on next page

4.2 Cardholder Registration, continued

When the CA receives the cardholder’s request, it decrypts the digital envelope to obtain the symmetric encryption key, the account information, and the random number generated by the cardholder software. It uses the symmetric key to decrypt the registration request. It then uses the signature key in the message to ensure the request was signed using the corresponding private signature key. If the signature is verified, the message processing continues; otherwise, the message is rejected and an appropriate response message is returned to the cardholder.

Next the CA must verify the information from the registration request using the cardholder’s account information. The process by which the CA and the Issuer exchange information and the steps taken to verify the information in the registration request are outside the scope of this specification. As described in Section 4.1, there are several ways to configure the processing performed by the CA and the Issuer, such as having the payment card brand provide some or all of the functions on behalf of the Issuer or having the Issuer provide all of the functions.

If the information in the registration request is verified, a certificate will be issued. First, the CA generates a random number that is combined with the random number created by the cardholder software to generate a secret value. This secret value is used to protect the account information in the cardholder certificate. The account number, expiration date, and the secret value are encoded using a one-way hashing algorithm. The result of the hashing algorithm is placed into the cardholder certificate. If the account number, expiration date, and the secret value are known, the link to the certificate can be proven, but the information cannot be derived by looking at the certificate.

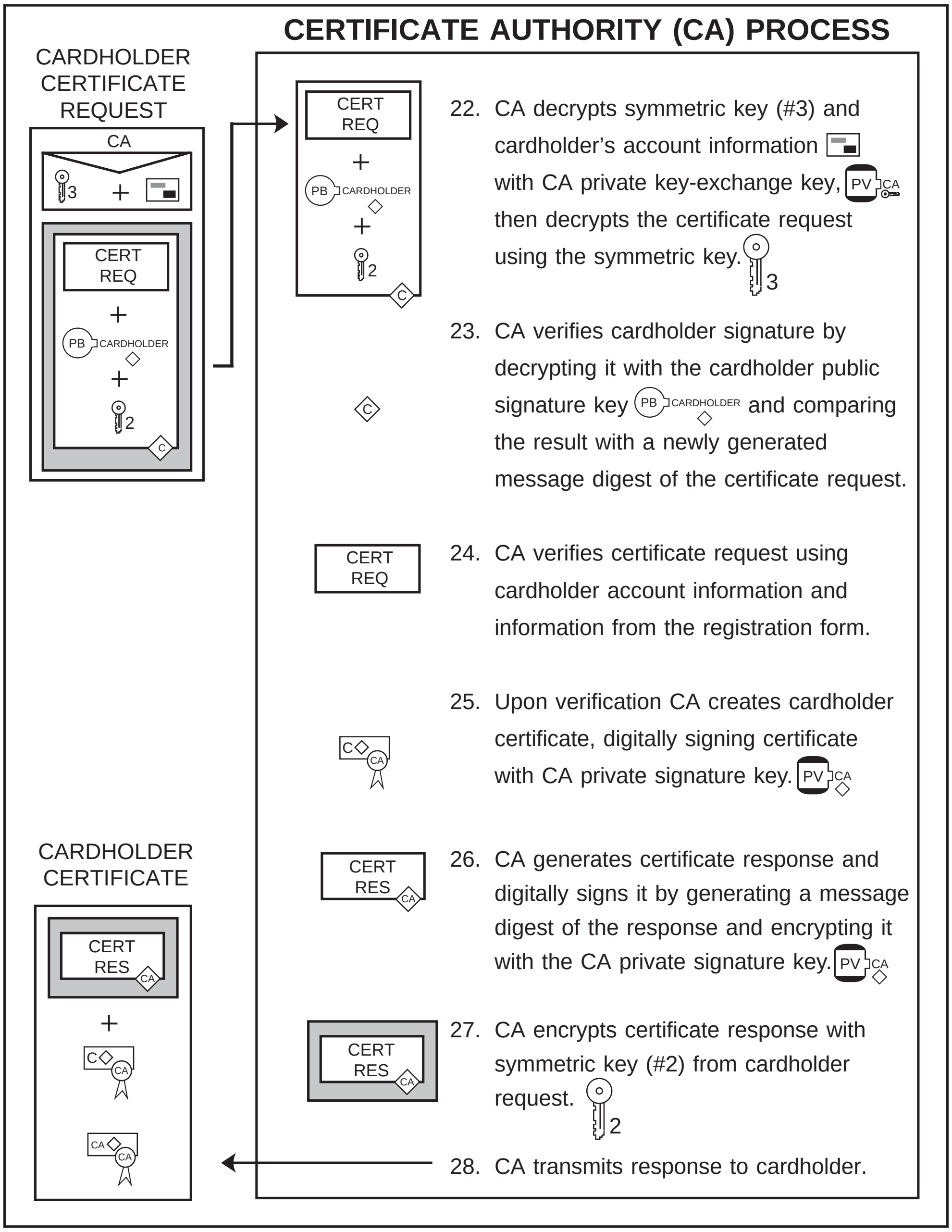
Next, the CA creates and digitally signs the cardholder certificate. The validity period of this certificate will be determined by CA policy; often it will correspond to the expiration date of the payment card, but it may expire sooner.

A response message containing the random number generated by the CA and other information (such as the brand logo) is then generated and encrypted using the symmetric key sent by the cardholder software in the registration message. The response is then transmitted to the cardholder.

Continued on next page

4.2 Cardholder Registration, continued

Certificate Authority processes request and creates certificate



CERTIFICATE AUTHORITY (CA) PROCESS

22. CA decrypts symmetric key (#3) and cardholder’s account information with CA private key-exchange key, PV CA then decrypts the certificate request using the symmetric key. 3

23. CA verifies cardholder signature by decrypting it with the cardholder public signature key PB CARDHOLDER and comparing the result with a newly generated message digest of the certificate request.

24. CA verifies certificate request using cardholder account information and information from the registration form.

25. Upon verification CA creates cardholder certificate, digitally signing certificate with CA private signature key. PV CA

26. CA generates certificate response and digitally signs it by generating a message digest of the response and encrypting it with the CA private signature key. PV CA

27. CA encrypts certificate response with symmetric key (#2) from cardholder request. 2

28. CA transmits response to cardholder.

Continued on next page

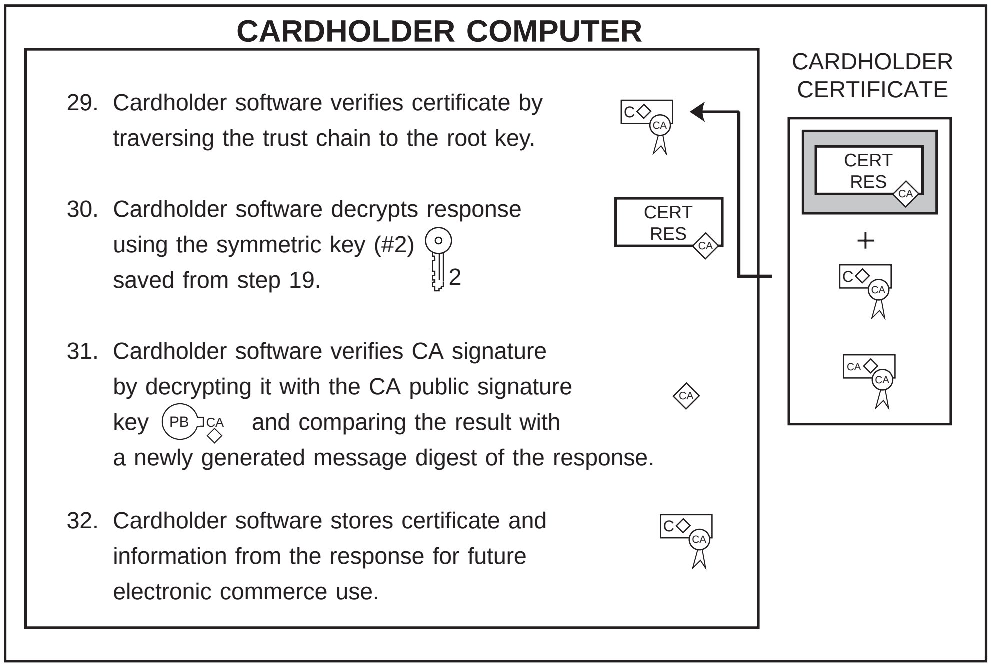
4.2 Cardholder Registration, continued

When the cardholder software receives the response from the CA, it verifies the certificate by traversing the trust chain to the root key, as described in Section 3.3. It stores the certificate on the cardholder's computer for use in future electronic commerce transactions.

Next, the cardholder software decrypts the registration response using the symmetric encryption key that it sent to the CA in the registration message. It combines the random number returned by the CA with the value that it sent in the registration message to determine the secret value. It then stores the secret value to use with the certificate.

Cardholder software vendors will ensure that the certificate and related information is stored in a way to prevent unauthorized access.

Cardholder receives certificate



CARDHOLDER COMPUTER

29. Cardholder software verifies certificate by traversing the trust chain to the root key.

30. Cardholder software decrypts response using the symmetric key (#2) saved from step 19.

31. Cardholder software verifies CA signature by decrypting it with the CA public signature key PB CA and comparing the result with a newly generated message digest of the response.

32. Cardholder software stores certificate and information from the response for future electronic commerce use.

4.3 Merchant Registration

Figure 7 provides a high-level overview of the merchant registration process, showing its five fundamental steps. The detailed sections that follow describe each step. The icon to the left corresponds to Figure 7 and serves as a map to the scenario; it is repeated in the more detailed sections with a shaded region that indicates which step is being described.

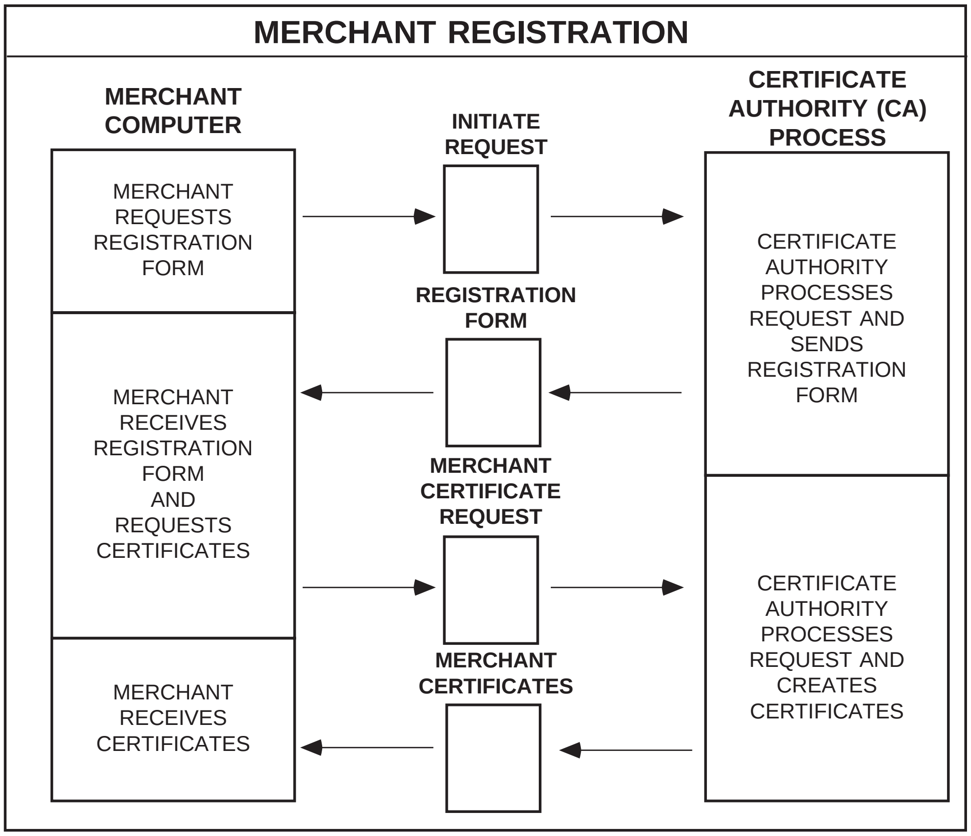

MERCHANT REGISTRATION
MERCHANT COMPUTER
CERTIFICATE AUTHORITY (CA) PROCESS
MERCHANT REQUESTS REGISTRATION FORM
INITIATE REQUEST
CERTIFICATE AUTHORITY PROCESSES REQUEST AND SENDS REGISTRATION FORM
REGISTRATION FORM
MERCHANT RECEIVES REGISTRATION FORM AND REQUESTS CERTIFICATES
MERCHANT CERTIFICATE REQUEST
CERTIFICATE AUTHORITY PROCESSES REQUEST AND CREATES CERTIFICATES
MERCHANT CERTIFICATES
MERCHANT RECEIVES CERTIFICATES

Figure 7: Merchant Registration

Continued on next page

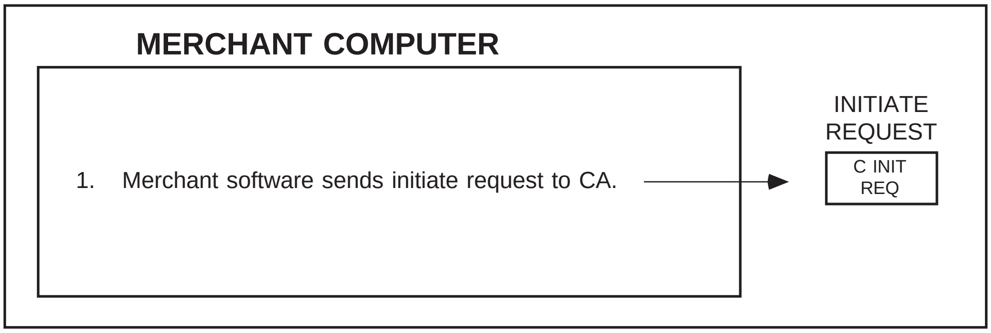
4.3 Merchant Registration, continued

Merchants must register with a Certificate Authority (CA) before they can receive SET payment instructions from cardholders or process SET transactions through a payment gateway. In order to send SET messages to the CA, the merchant must have a copy of the CA public key-exchange key, which is provided in the CA key-exchange certificate.

The merchant also needs a copy of the registration form from the merchant's financial institution. The merchant software must identify the Acquirer to the CA.

The registration process starts when the merchant software requests a copy of the CA's key-exchange certificate and the appropriate registration form.

Merchant requests registration form



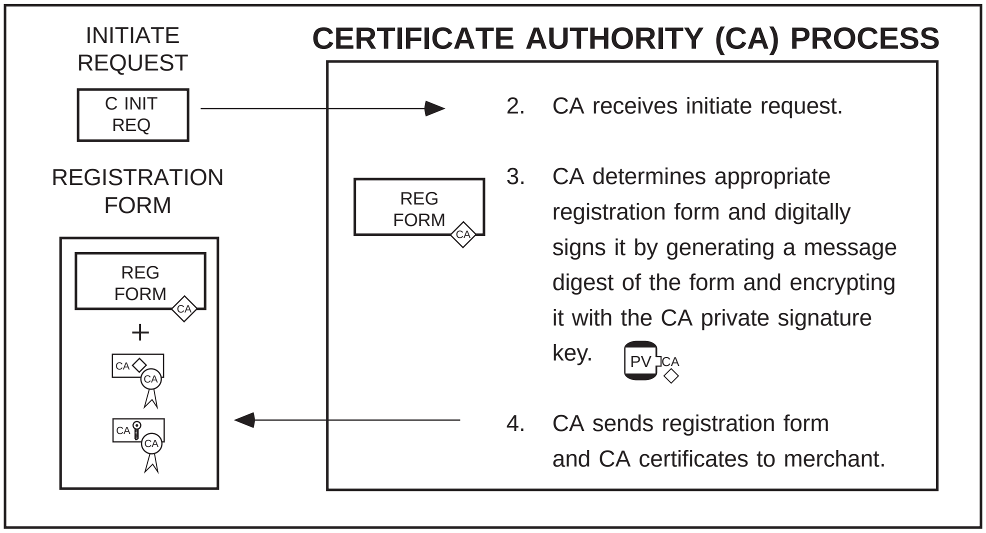
1. Merchant software sends initiate request to CA.

Continued on next page

4.3 Merchant Registration, continued

The CA identifies the merchant’s financial institution and selects the appropriate registration form. It returns this registration form along with a copy of its own key-exchange certificate to the merchant.

Certificate Authority processes request and sends registration form



2. CA receives initiate request.
3. CA determines appropriate registration form and digitally signs it by generating a message digest of the form and encrypting it with the CA private signature key.
4. CA sends registration form and CA certificates to merchant.

Continued on next page

4.3 Merchant Registration, continued

The merchant software verifies the CA certificate by traversing the trust chain to the root key, then holds the CA certificate to use later during the registration process. Once the software has a copy of the CA key-exchange certificate, the merchant can register to accept SET payment instructions and process SET transactions. The merchant must have a relationship with an Acquirer that processes SET transactions before a certificate request can be processed.

The merchant needs two public/private key pairs for use with SET: key-exchange and signature. The merchant software generates these key pairs if they do not already exist.

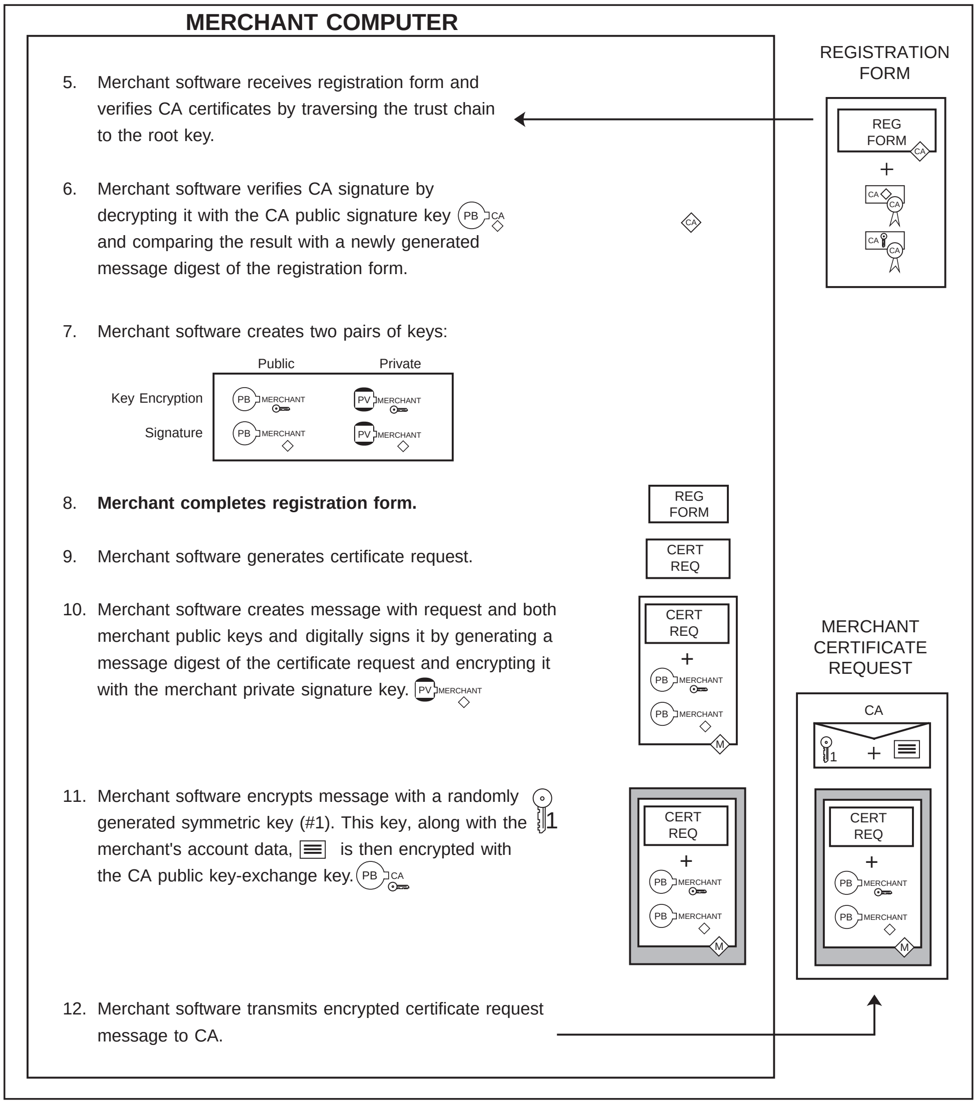
To register, the merchant fills out the registration form on the screen with information such as the merchant’s name, address, and merchant ID.

The merchant software takes this registration information and combines it with the public keys in a registration message. The software digitally signs the registration message. Next the software generates a random symmetric encryption key. It uses this random key to encrypt the message. The random key is then encrypted into the digital envelope using the CA public key-exchange key. Finally, the software transmits all of these components to the CA.

Continued on next page

4.3 Merchant Registration, continued

Merchant receives registration form and requests certificates



MERCHANT COMPUTER

5. Merchant software receives registration form and verifies CA certificates by traversing the trust chain to the root key.

6. Merchant software verifies CA signature by decrypting it with the CA public signature key PB CA and comparing the result with a newly generated message digest of the registration form.

7. Merchant software creates two pairs of keys:

	Public	Private
Key Encryption	PB MERCHANT	PV MERCHANT
Signature	PB MERCHANT	PV MERCHANT

8. **Merchant completes registration form.**

9. Merchant software generates certificate request.

10. Merchant software creates message with request and both merchant public keys and digitally signs it by generating a message digest of the certificate request and encrypting it with the merchant private signature key. PV MERCHANT

11. Merchant software encrypts message with a randomly generated symmetric key (#1). This key, along with the merchant's account data, is then encrypted with the CA public key-exchange key. PB CA

12. Merchant software transmits encrypted certificate request message to CA.

Continued on next page

4.3 Merchant Registration, continued

When the CA receives the merchant’s request, it decrypts the digital envelope to obtain the symmetric encryption key, which it uses to decrypt the registration request. It then uses the signature key in the message to ensure that the request was signed using the corresponding private signature key. If the signature is verified, the message processing continues; otherwise, the message is rejected and an appropriate response message is returned to the merchant.

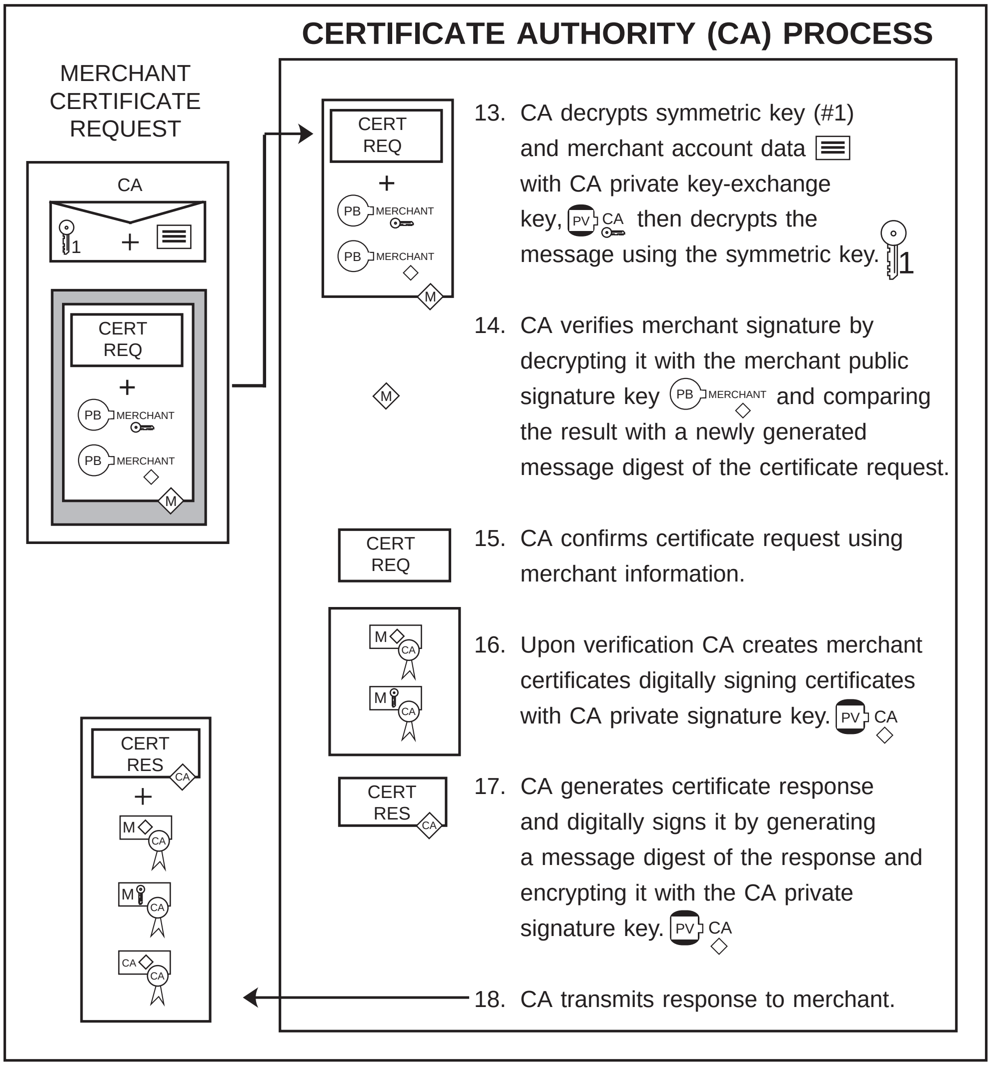
Next the CA must verify the information from the registration request using known merchant information. The process by which the CA and the Acquirer exchange information and the steps taken to verify the information in the registration request are outside the scope of this specification. As described in Section 4.1, there are several ways to configure the processing performed by the CA and the Acquirer, such as having the payment card brand provide some or all of the functions on behalf of the Acquirer or having the Acquirer provide all of the functions.

If the information in the registration request is verified, the CA creates and digitally signs the merchant certificates. The validity period of these certificates will be determined by CA policy; often it will correspond to the expiration date of the merchant’s contract with the Acquirer, but it may expire sooner. The certificates are then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the merchant public key-exchange key. The response is then transmitted to the merchant.

Continued on next page

4.3 Merchant Registration, continued

Certificate Authority processes request and creates certificates



CERTIFICATE AUTHORITY (CA) PROCESS

13. CA decrypts symmetric key (#1) and merchant account data with CA private key-exchange key, PV CA then decrypts the message using the symmetric key. 1

14. CA verifies merchant signature by decrypting it with the merchant public signature key PB MERCHANT and comparing the result with a newly generated message digest of the certificate request.

15. CA confirms certificate request using merchant information.

16. Upon verification CA creates merchant certificates digitally signing certificates with CA private signature key. PV CA

17. CA generates certificate response and digitally signs it by generating a message digest of the response and encrypting it with the CA private signature key. PV CA

18. CA transmits response to merchant.

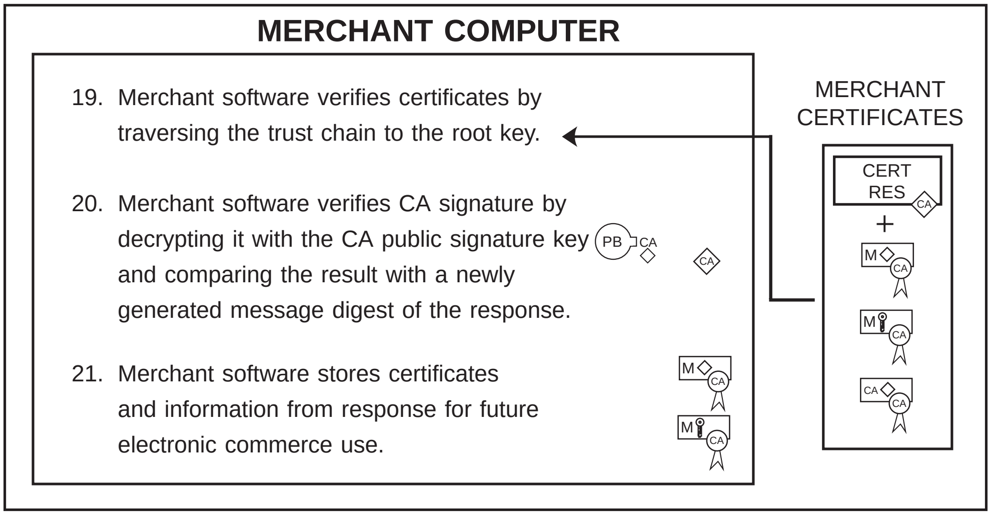
Continued on next page

4.3 Merchant Registration, continued

When the merchant software receives the response from the CA, it decrypts the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypt the registration response containing the merchant certificates.

After the merchant software verifies the certificates by traversing the trust chain to the root key, it stores the certificates on the merchant's computer for use in future electronic commerce transactions.

Merchant receives certificates



19. Merchant software verifies certificates by traversing the trust chain to the root key.

20. Merchant software verifies CA signature by decrypting it with the CA public signature key and comparing the result with a newly generated message digest of the response.

21. Merchant software stores certificates and information from response for future electronic commerce use.

4.4 Purchase Request

Figure 8 provides a high level overview of the purchase request portion of a cardholder’s order process, showing its five fundamental steps. The detailed sections that follow describe each step. The icon to the left corresponds to Figure 8 and serves as a map to the scenario; it is repeated in the more detailed sections with a shaded region that indicates which step is being described.

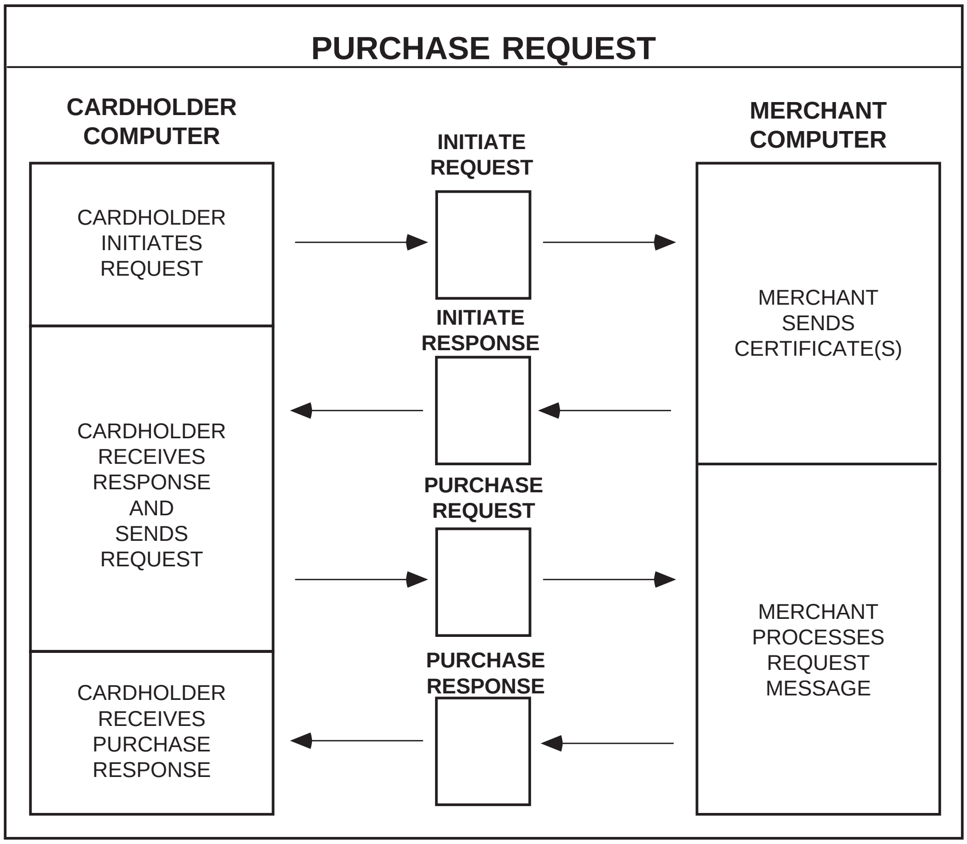

PURCHASE REQUEST
CARDHOLDER COMPUTER
MERCHANT COMPUTER
CARDHOLDER INITIATES REQUEST
INITIATE REQUEST
MERCHANT SENDS CERTIFICATE(S)
INITIATE RESPONSE
CARDHOLDER RECEIVES RESPONSE AND SENDS REQUEST
PURCHASE REQUEST
MERCHANT PROCESSES REQUEST MESSAGE
PURCHASE RESPONSE
CARDHOLDER RECEIVES PURCHASE RESPONSE

Figure 8: Purchase Request

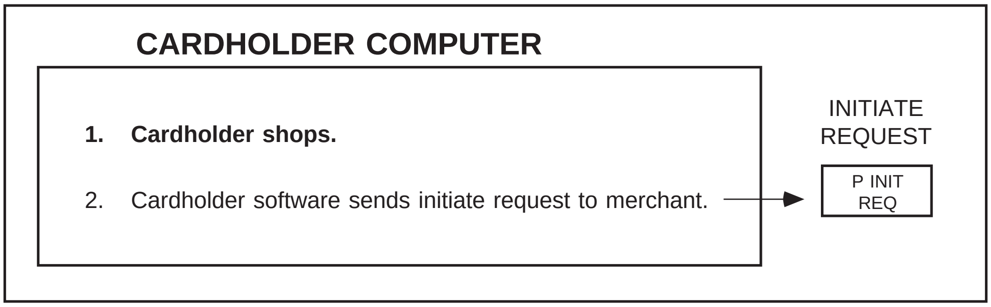
Continued on next page

4.4 Purchase Request, continued

The SET protocol is invoked after the cardholder has completed browsing, selection, and ordering. Before this flow begins, the cardholder will have been presented with a completed order form and approved its contents and terms, such as the number of installment payments if the merchant is billing for the transaction in installments. In addition, the cardholder will have selected a payment card as the means of payment.

In order to send SET messages to a merchant, the cardholder must have a copy of the Payment Gateway's key-exchange keys. The SET order process is started when the cardholder software requests a copy of the gateway's certificate. The message from the cardholder indicates which payment card brand will be used for the transaction.

Cardholder initiates request



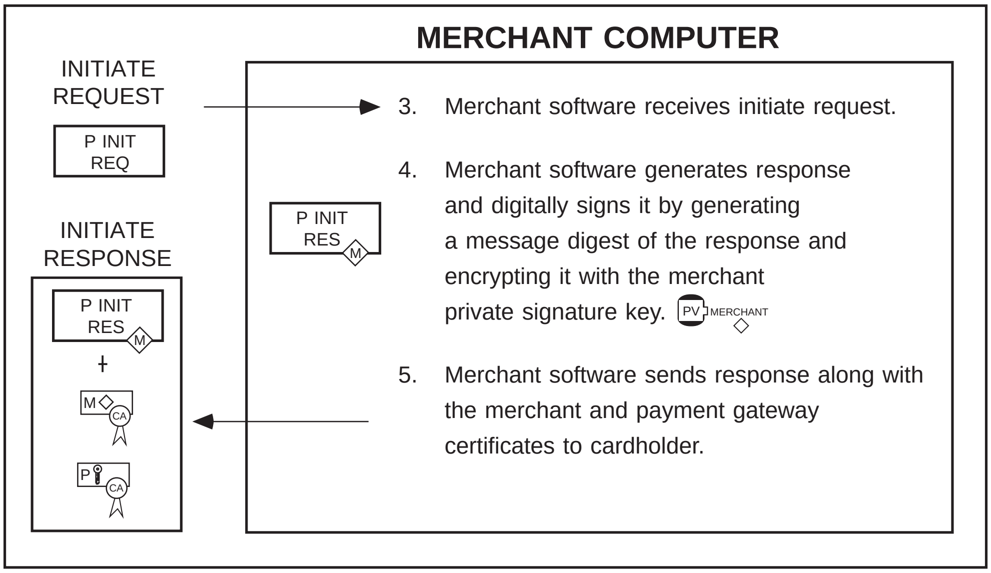
1. **Cardholder shops.**
2. Cardholder software sends initiate request to merchant.

Continued on next page

4.4 Purchase Request, continued

When the merchant receives the request, it assigns a unique transaction identifier to the message. It then transmits the merchant and gateway certificates that correspond to the payment card brand indicated by the cardholder, along with the transaction identifier to the cardholder.

Merchant sends certificate(s)



MERCHANT COMPUTER

3. Merchant software receives initiate request.

4. Merchant software generates response and digitally signs it by generating a message digest of the response and encrypting it with the merchant private signature key.

5. Merchant software sends response along with the merchant and payment gateway certificates to cardholder.

Continued on next page

4.4 Purchase Request, continued

The cardholder software verifies the merchant and gateway certificates by traversing the trust chain to the root key, then holds these certificates to use later during the ordering process.

The cardholder software creates the Order Information (OI) and Payment Instructions (PI). The software places the transaction identifier assigned by the merchant in the OI and the PI; this identifier will be used by the Payment Gateway to link the OI and the PI together when the merchant requests authorization.

Note: The OI does not contain the order data such as the description of goods (the items and quantities) or the terms of the order (such as number of installment payments). This information is exchanged between the cardholder and merchant software during the shopping phase before the first SET message.

The cardholder software generates a dual signature for the OI and the PI by computing the message digests of both, concatenating the two digests, computing the message digest of the result and encrypting that using the cardholder private signature key. The message digests of the OI and the PI are sent along with the dual signature.

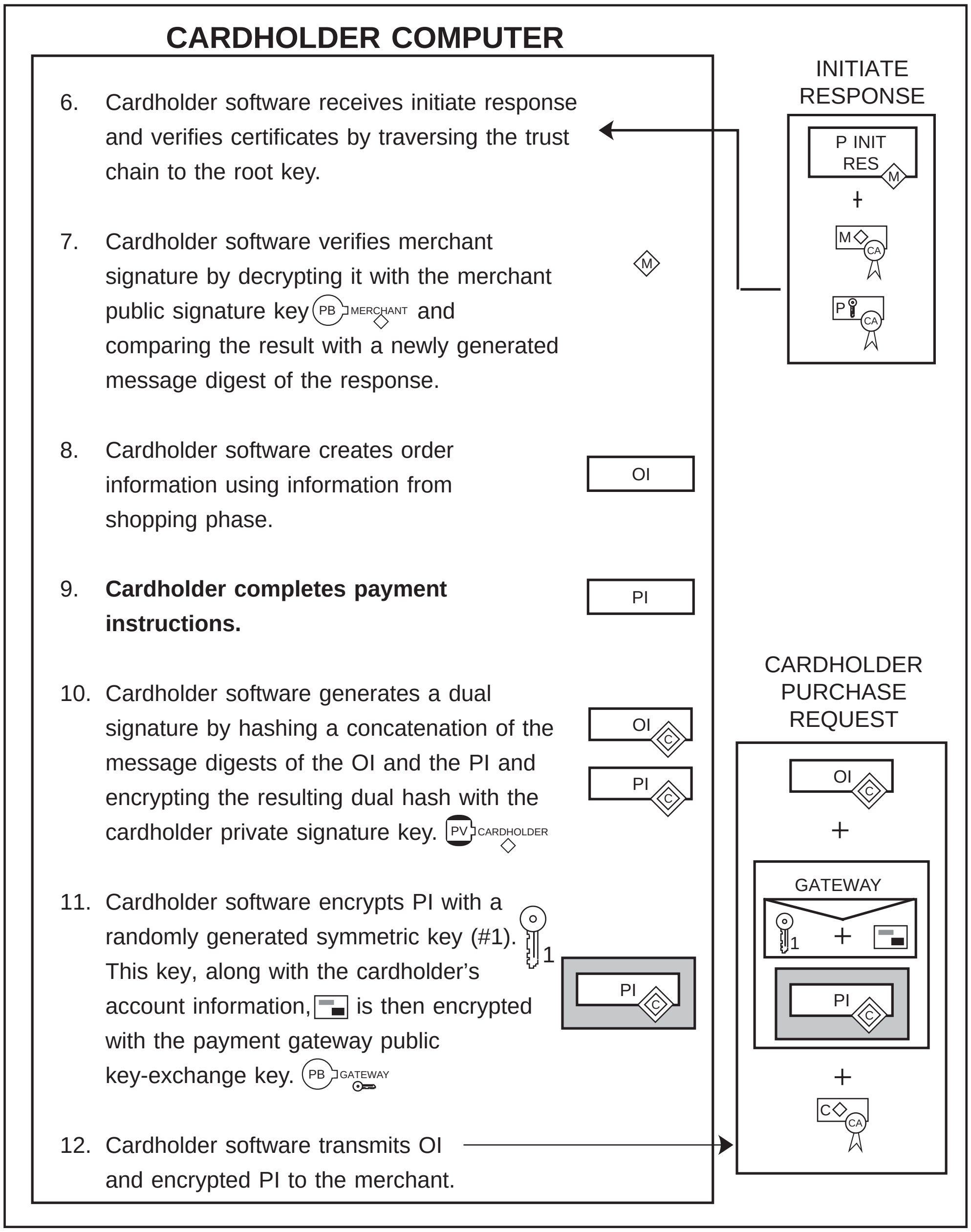
Next the software generates a random symmetric encryption key and uses it to encrypt the dual signed PI. The software then encrypts the cardholder account number as well as the random symmetric key used to encrypt the PI into a digital envelope using the Payment Gateway’s key-exchange key.

Finally, the software transmits a message consisting of the OI and the PI to the merchant.

Continued on next page

4.4 Purchase Request, continued

Cardholder receives response and sends request



CARDHOLDER COMPUTER

6. Cardholder software receives initiate response and verifies certificates by traversing the trust chain to the root key.

7. Cardholder software verifies merchant signature by decrypting it with the merchant public signature key PB MERCHANT and comparing the result with a newly generated message digest of the response.

8. Cardholder software creates order information using information from shopping phase.

9. **Cardholder completes payment instructions.**

10. Cardholder software generates a dual signature by hashing a concatenation of the message digests of the OI and the PI and encrypting the resulting dual hash with the cardholder private signature key. PV CARDHOLDER

11. Cardholder software encrypts PI with a randomly generated symmetric key (#1). This key, along with the cardholder's account information, ▬ is then encrypted with the payment gateway public key-exchange key. PB GATEWAY

12. Cardholder software transmits OI and encrypted PI to the merchant.

Continued on next page

4.4 Purchase Request, continued

When the merchant software receives the order, it verifies the cardholder signature certificate by traversing the trust chain to the root key. Next it uses the cardholder public signature key and the message digest of the PI (included with the OI) to check the digital signature to ensure that the order has not been tampered with in transit and that it was signed using the cardholder private signature key.

The merchant software then processes the order including the payment authorization described in Section 4.5.

Note: It is not necessary for the merchant to perform the authorization phase prior to sending a response to the cardholder. The cardholder can determine later if the authorization has been performed by sending an order inquiry message. (The order inquiry flow is described in Book 2: Programmer’s Guide.)

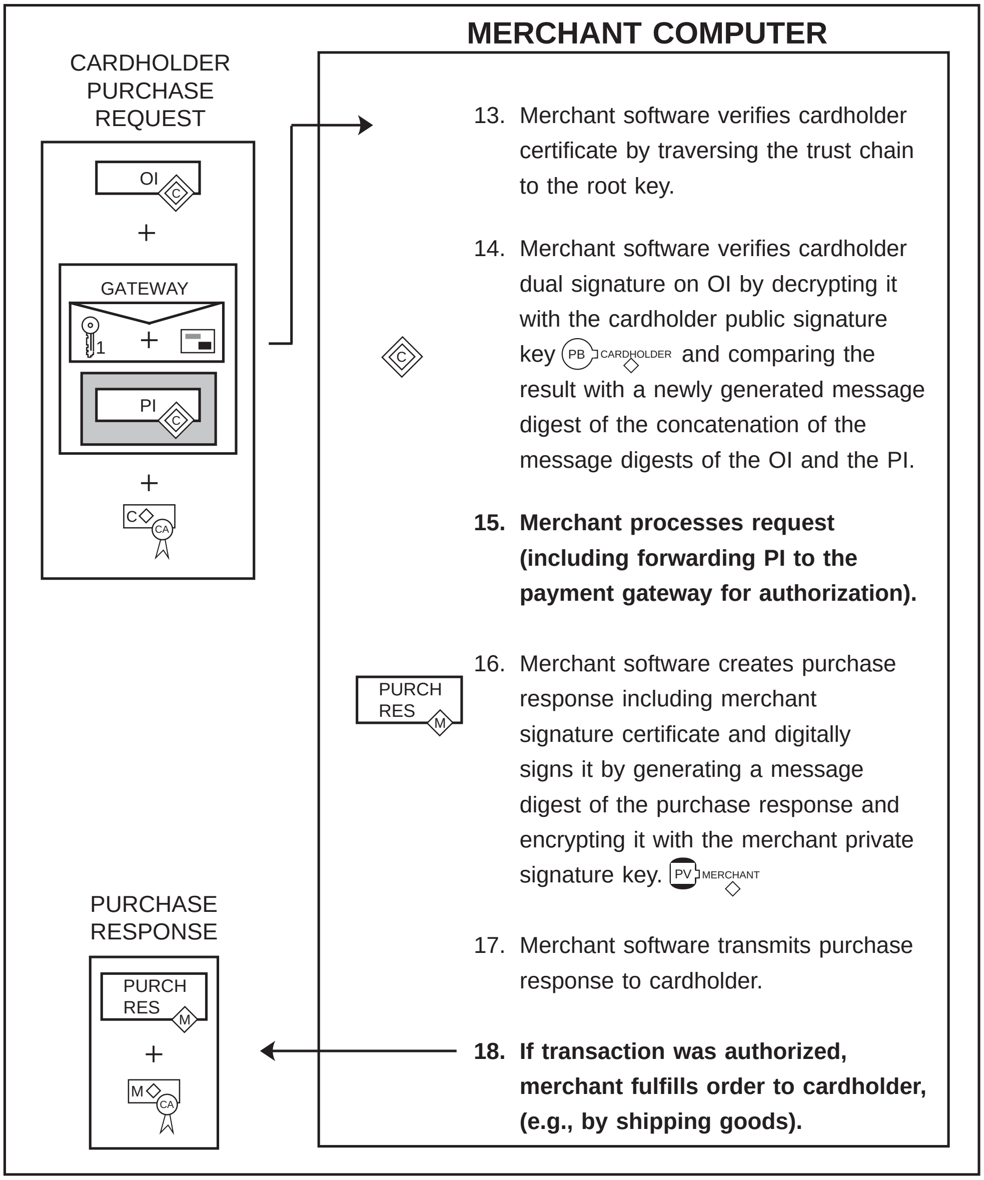
After the OI has been processed, the merchant software generates and digitally signs a purchase response message, which includes the merchant signature certificate and indicates that the cardholder’s order has been received by the merchant. The response is then transmitted to the cardholder.

If the authorization response (see Section 4.5) indicates that the transaction was approved, the merchant will ship the goods or perform the services indicated in the order.

Continued on next page

4.4 Purchase Request, continued

Merchant processes request message



13. Merchant software verifies cardholder certificate by traversing the trust chain to the root key.

14. Merchant software verifies cardholder dual signature on OI by decrypting it with the cardholder public signature key PB CARDHOLDER and comparing the result with a newly generated message digest of the concatenation of the message digests of the OI and the PI.

15. Merchant processes request (including forwarding PI to the payment gateway for authorization).

16. Merchant software creates purchase response including merchant signature certificate and digitally signs it by generating a message digest of the purchase response and encrypting it with the merchant private signature key. PV MERCHANT

17. Merchant software transmits purchase response to cardholder.

18. If transaction was authorized, merchant fulfills order to cardholder, (e.g., by shipping goods).

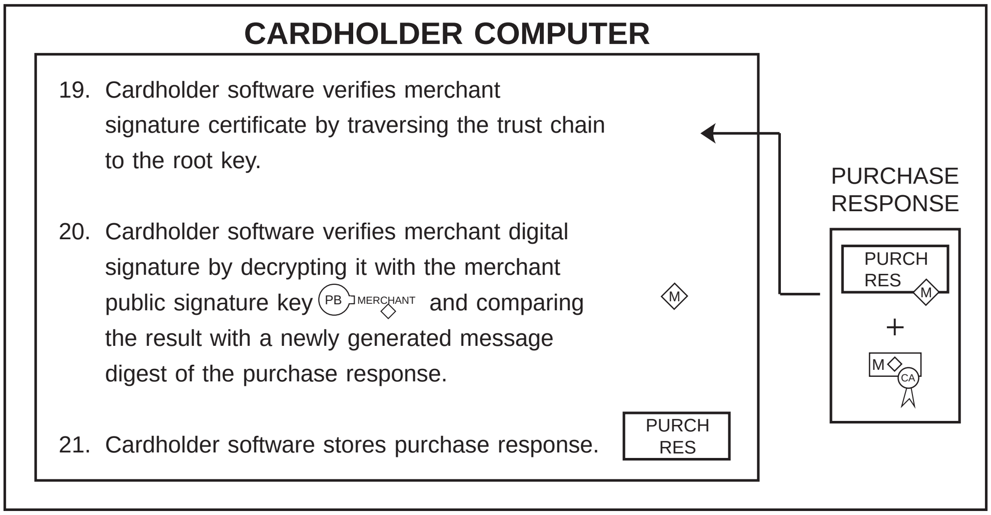
Continued on next page

4.4 Purchase Request, continued

When the cardholder software receives the purchase response message from the merchant, it verifies the merchant signature certificate by traversing the trust chain to the root key. It uses the merchant public signature key to check the merchant's digital signature. Finally, it takes some action based on the contents of the response message, such as displaying a message to the cardholder or updating a database with the status of the order.

The cardholder can determine the status of the order (such as whether it has been authorized or submitted for payment) by sending an order inquiry message. This message is described in Book 2: Programmer's Guide.

Cardholder receives purchase response


CARDHOLDER COMPUTER

19. Cardholder software verifies merchant signature certificate by traversing the trust chain to the root key.

20. Cardholder software verifies merchant digital signature by decrypting it with the merchant public signature key PB MERCHANT and comparing the result with a newly generated message digest of the purchase response.

21. Cardholder software stores purchase response.

4.5 Payment Authorization

Figure 9 provides a high level overview of a merchant's payment authorization process, showing its three fundamental steps. The detailed sections that follow describe each step. The icon to the left corresponds to Figure 9 and serves as a map to the scenario; it is repeated in the more detailed sections with a shaded region that indicates which step is being described.

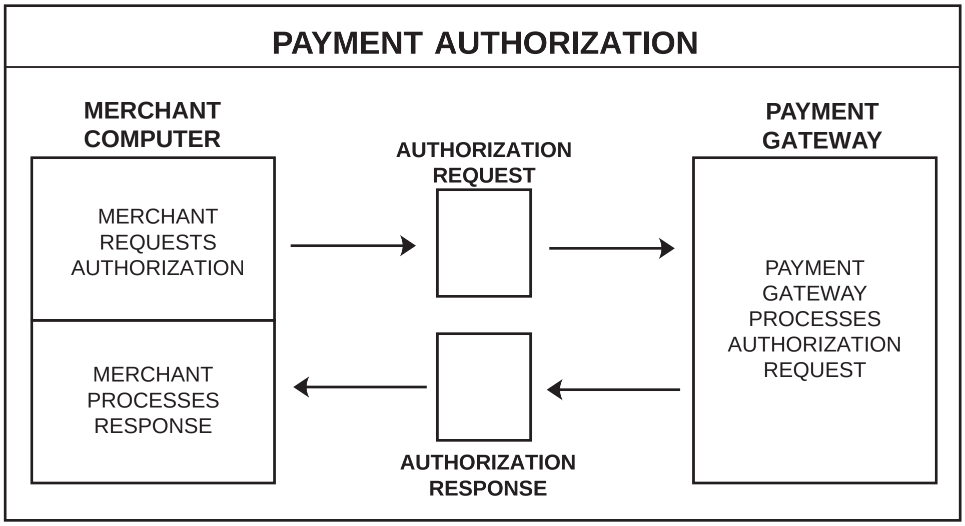

PAYMENT AUTHORIZATION
MERCHANT COMPUTER
MERCHANT REQUESTS AUTHORIZATION
MERCHANT PROCESSES RESPONSE
AUTHORIZATION REQUEST
AUTHORIZATION RESPONSE
PAYMENT GATEWAY
PAYMENT GATEWAY PROCESSES AUTHORIZATION REQUEST

Figure 9: Payment Authorization

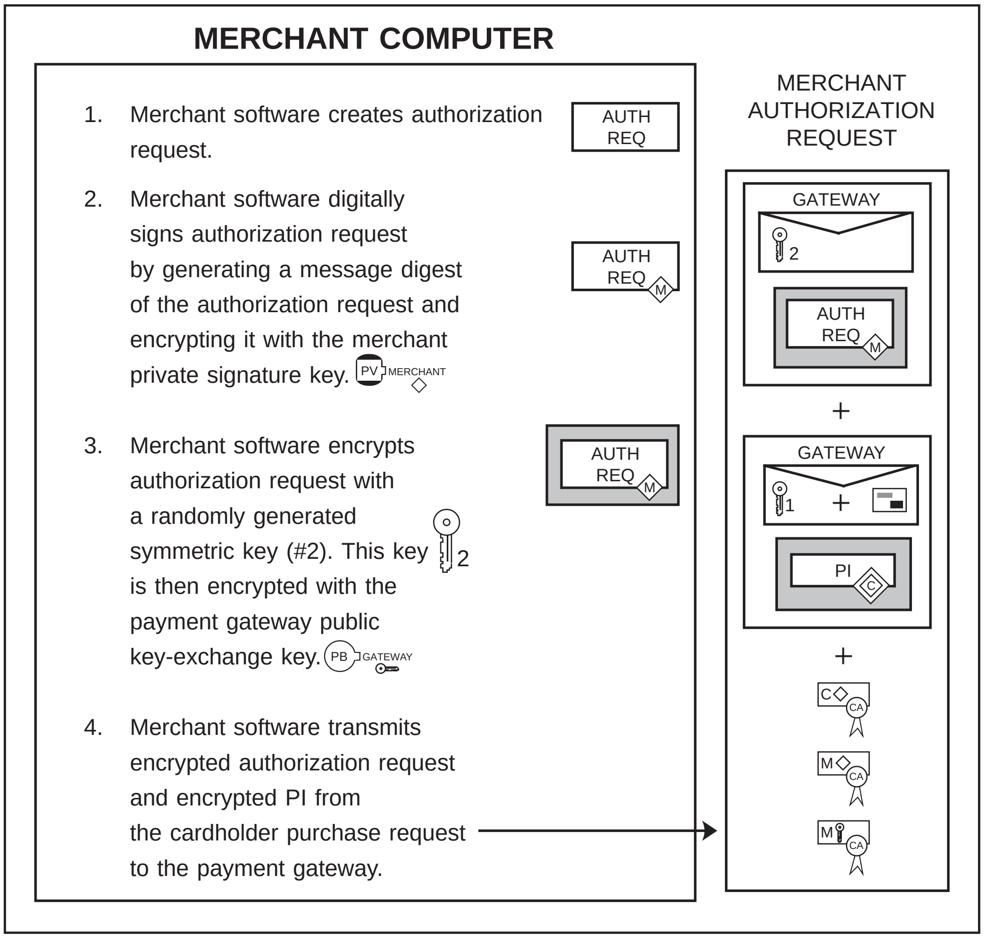
Continued on next page

4.5 Payment Authorization, continued

During the processing of an order from a cardholder (see Section 4.4), the merchant will authorize the transaction. The merchant software generates and digitally signs an authorization request, which includes the amount to be authorized, the transaction identifier from the OI, and other information about the transaction. The request is then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the public key-exchange key of the Payment Gateway. (This is the same key the cardholder used to encrypt the digital envelope of the payment instructions.) The authorization request and the cardholder payment instructions are then transmitted to the Payment Gateway.

Note: The SET protocol also includes a sales transaction that allows a merchant to authorize a transaction and request payment in a single message. While the sales message includes an additional block of data on the request from the merchant, it otherwise parallels the message flow described in this section. Details about the processing of a sales transaction are provided in Book 2: Programmer’s Guide.

Merchant requests authorization



1. Merchant software creates authorization request.
2. Merchant software digitally signs authorization request by generating a message digest of the authorization request and encrypting it with the merchant private signature key.
3. Merchant software encrypts authorization request with a randomly generated symmetric key (#2). This key is then encrypted with the payment gateway public key-exchange key.
4. Merchant software transmits encrypted authorization request and encrypted PI from the cardholder purchase request to the payment gateway.

Continued on next page

4.5 Payment Authorization, continued

When the Payment Gateway receives the authorization request, it decrypts the digital envelope of the authorization request to obtain the symmetric encryption key. It uses the symmetric key to decrypt the request. It then verifies the merchant signature certificate by traversing the trust chain to the root key; it also verifies that the certificate has not expired. It uses the merchant public signature key to ensure the request was signed using the merchant private signature key.

Next the Payment Gateway decrypts the digital envelope of the Payment Instructions to obtain the symmetric encryption key and the account information. It uses the symmetric key to decrypt the PI. It then verifies the cardholder signature certificate by traversing the trust chain to the root; it also verifies that the certificate has not expired. Next it uses the cardholder public signature key and the message digest of the OI (included in the PI) to check the digital signature to ensure that the PI has not been tampered with in transit and that it was signed using the cardholder private signature key.

Next, the Payment Gateway verifies that the transaction identifier received from the merchant matches the one in the cardholder Payment Instructions. The Payment Gateway then formats and sends an authorization request to the Issuer via a payment system.

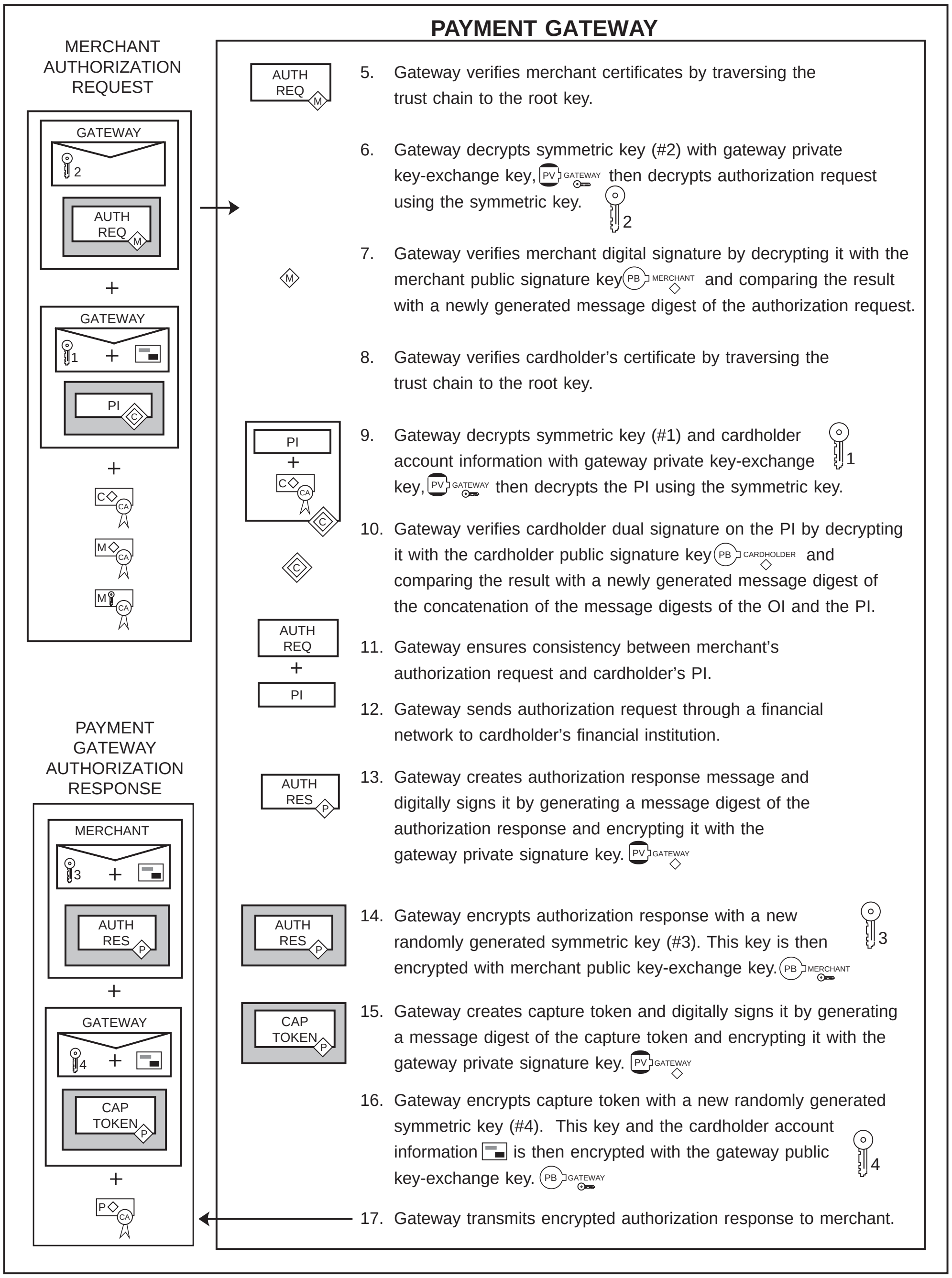
Upon receiving an authorization response from the Issuer, the Payment Gateway generates and digitally signs an authorization response message, which includes the Issuer's response and a copy of the Payment Gateway signature certificate. The response also includes an optional capture token with information the Payment Gateway will need to process a capture request (see Section 4.6). The capture token is only included if required by the Acquirer.

The response is then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the merchant public key-exchange key. The response is then transmitted to the merchant.

Continued on next page

4.5 Payment Authorization, continued

Payment Gateway processes authorization request



5. Gateway verifies merchant certificates by traversing the trust chain to the root key.

6. Gateway decrypts symmetric key (#2) with gateway private key-exchange key, PV GATEWAY then decrypts authorization request using the symmetric key. 2

7. Gateway verifies merchant digital signature by decrypting it with the merchant public signature key PB MERCHANT and comparing the result with a newly generated message digest of the authorization request.

8. Gateway verifies cardholder's certificate by traversing the trust chain to the root key.

9. Gateway decrypts symmetric key (#1) and cardholder account information with gateway private key-exchange key, PV GATEWAY then decrypts the PI using the symmetric key. 1

10. Gateway verifies cardholder dual signature on the PI by decrypting it with the cardholder public signature key PB CARDHOLDER and comparing the result with a newly generated message digest of the concatenation of the message digests of the OI and the PI.

11. Gateway ensures consistency between merchant's authorization request and cardholder's PI.

12. Gateway sends authorization request through a financial network to cardholder's financial institution.

13. Gateway creates authorization response message and digitally signs it by generating a message digest of the authorization response and encrypting it with the gateway private signature key. PV GATEWAY

14. Gateway encrypts authorization response with a new randomly generated symmetric key (#3). This key is then encrypted with merchant public key-exchange key. PB MERCHANT 3

15. Gateway creates capture token and digitally signs it by generating a message digest of the capture token and encrypting it with the gateway private signature key. PV GATEWAY

16. Gateway encrypts capture token with a new randomly generated symmetric key (#4). This key and the cardholder account information ▬ is then encrypted with the gateway public key-exchange key. PB GATEWAY 4

17. Gateway transmits encrypted authorization response to merchant.

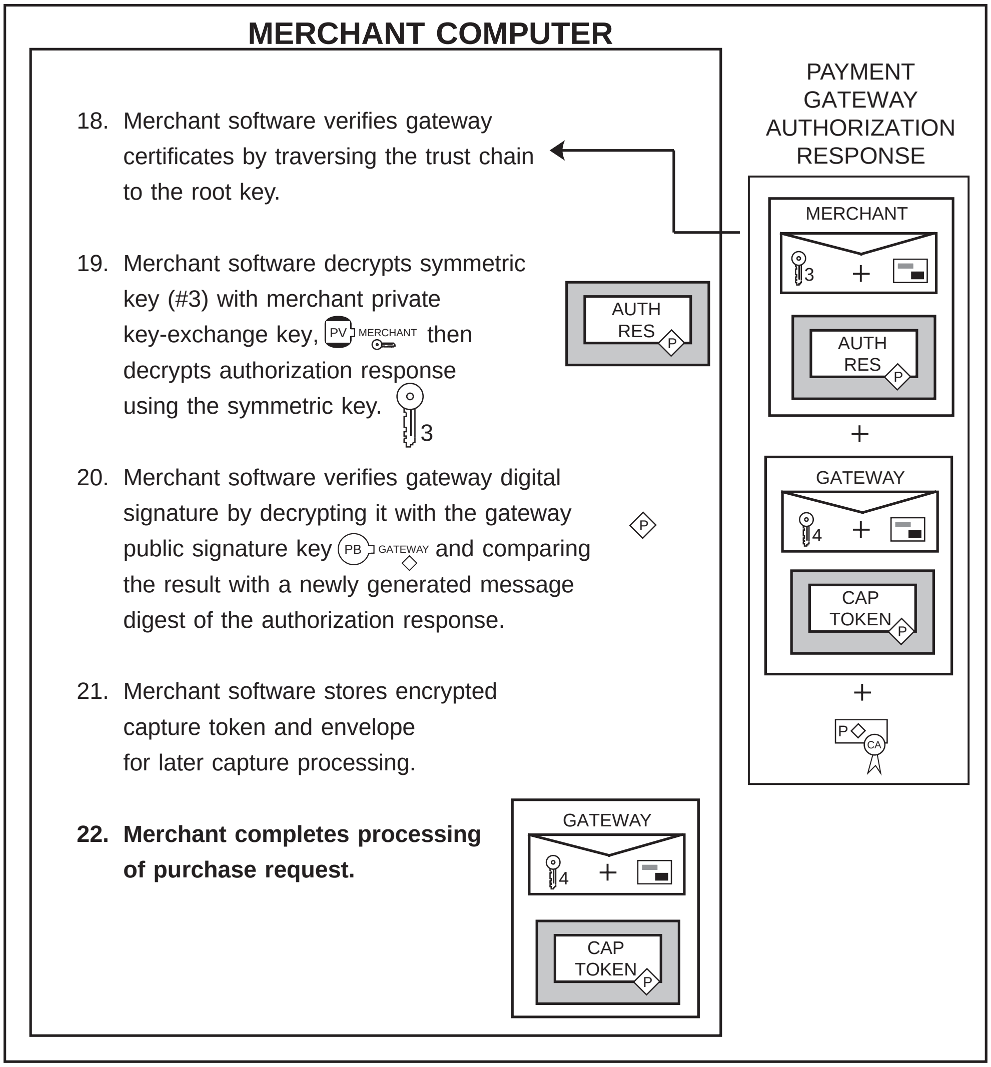
Continued on next page

4.5 Payment Authorization, continued

When the merchant software receives the authorization response message from the Payment Gateway, it decrypts the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypt the response message. It then verifies the Payment Gateway signature certificate by traversing the trust chain to the root key. It uses the Payment Gateway public signature key to check the Payment Gateway digital signature.

The merchant software stores the authorization response and the capture token to be used when requesting payment through a capture request (see Section 4.6). The merchant then completes processing of the cardholder's order (see Section 4.4) by shipping the goods or performing the services indicated in the order.

Merchant processes response



MERCHANT COMPUTER

18. Merchant software verifies gateway certificates by traversing the trust chain to the root key.

19. Merchant software decrypts symmetric key (#3) with merchant private key-exchange key, PV MERCHANT then decrypts authorization response using the symmetric key. 3

20. Merchant software verifies gateway digital signature by decrypting it with the gateway public signature key PB GATEWAY and comparing the result with a newly generated message digest of the authorization response.

21. Merchant software stores encrypted capture token and envelope for later capture processing.

22. Merchant completes processing of purchase request.

4.6 Payment Capture

Figure 10 provides a high level overview of a merchant’s payment capture process, showing its three fundamental steps. The detailed sections that follow describe each step. The icon to the left corresponds to Figure 10 and serves as a map to the scenario; it is repeated in the more detailed sections with a shaded region that indicates which step is being described.

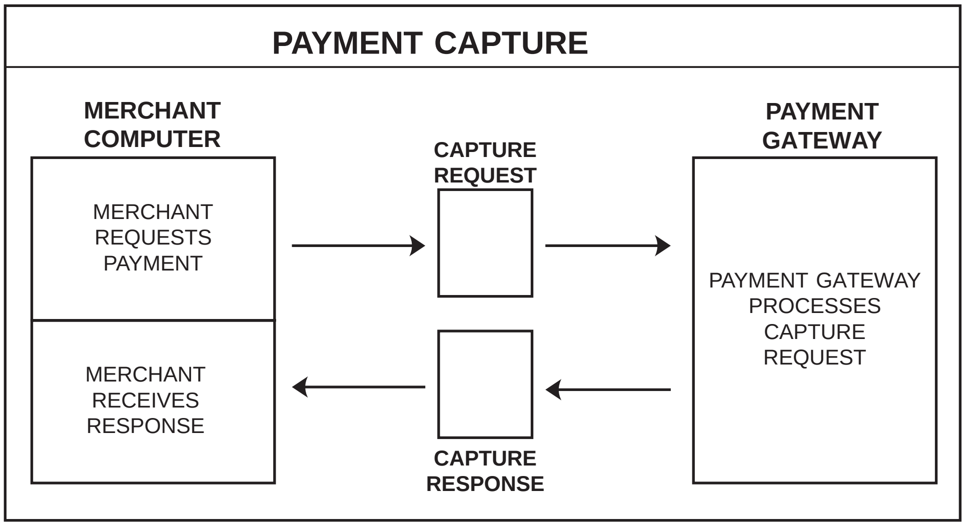

PAYMENT CAPTURE
MERCHANT COMPUTER
MERCHANT REQUESTS PAYMENT
MERCHANT RECEIVES RESPONSE
CAPTURE REQUEST
CAPTURE RESPONSE
PAYMENT GATEWAY
PAYMENT GATEWAY PROCESSES CAPTURE REQUEST

Figure 10: Payment Capture

Continued on next page

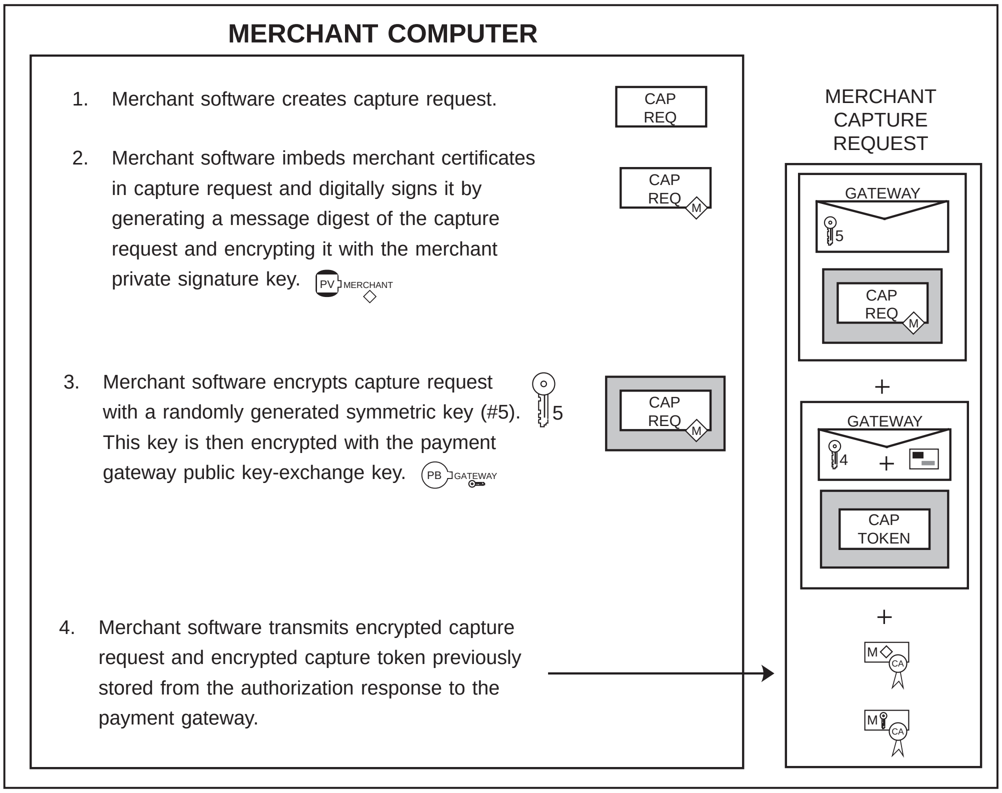
4.6 Payment Capture, continued

After completing the processing of an order from a cardholder (see Section 4.4), the merchant will request payment. There will often be a significant time lapse between the message requesting authorization and the message requesting payment.

The merchant software generates and digitally signs a capture request, which includes the final amount of the transaction, the transaction identifier from the OI, and other information about the transaction. The request is then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the public key-exchange key of the Payment Gateway. The capture request and optionally the capture token if one was included in the authorization response (see Section 4.5) are then transmitted to the Payment Gateway.

Note: While the flow described here contains only a single capture request, the merchant software is permitted to batch multiple requests into a single message.

Merchant requests payment



MERCHANT COMPUTER

1. Merchant software creates capture request.
2. Merchant software imbeds merchant certificates in capture request and digitally signs it by generating a message digest of the capture request and encrypting it with the merchant private signature key.
3. Merchant software encrypts capture request with a randomly generated symmetric key (#5). This key is then encrypted with the payment gateway public key-exchange key.
4. Merchant software transmits encrypted capture request and encrypted capture token previously stored from the authorization response to the payment gateway.

Continued on next page

4.6 Payment Capture, continued

When the Payment Gateway receives the capture request, it decrypts the digital envelope of the capture request to obtain the symmetric encryption key. It uses the symmetric key to decrypt the request. It then uses the merchant public signature key to ensure the request was signed using the merchant private signature key.

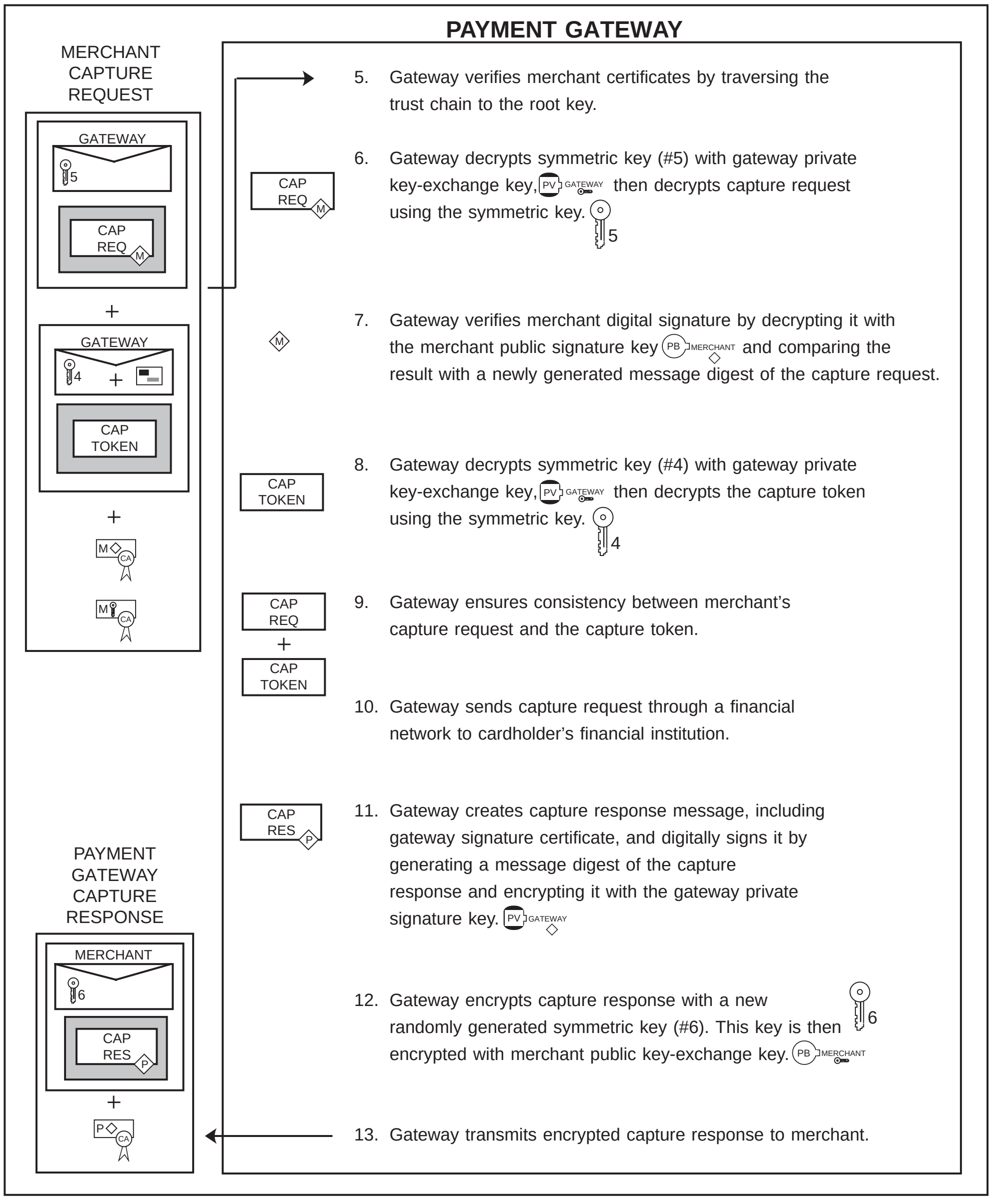
The Payment Gateway decrypts the capture token (if present) and then uses the information from the capture request and the capture token to format a clearing request, which it sends to the Issuer via a payment card payment system.

The Payment Gateway then generates and digitally signs a capture response message, which includes a copy of the Payment Gateway signature certificate. The response is then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the merchant public key-exchange key. The response is then transmitted to the merchant.

Continued on next page

4.6 Payment Capture, continued

Payment Gateway processes capture request



5. Gateway verifies merchant certificates by traversing the trust chain to the root key.

6. Gateway decrypts symmetric key (#5) with gateway private key-exchange key, then decrypts capture request using the symmetric key.

7. Gateway verifies merchant digital signature by decrypting it with the merchant public signature key and comparing the result with a newly generated message digest of the capture request.

8. Gateway decrypts symmetric key (#4) with gateway private key-exchange key, then decrypts the capture token using the symmetric key.

9. Gateway ensures consistency between merchant's capture request and the capture token.

10. Gateway sends capture request through a financial network to cardholder's financial institution.

11. Gateway creates capture response message, including gateway signature certificate, and digitally signs it by generating a message digest of the capture response and encrypting it with the gateway private signature key.

12. Gateway encrypts capture response with a new randomly generated symmetric key (#6). This key is then encrypted with merchant public key-exchange key.

13. Gateway transmits encrypted capture response to merchant.

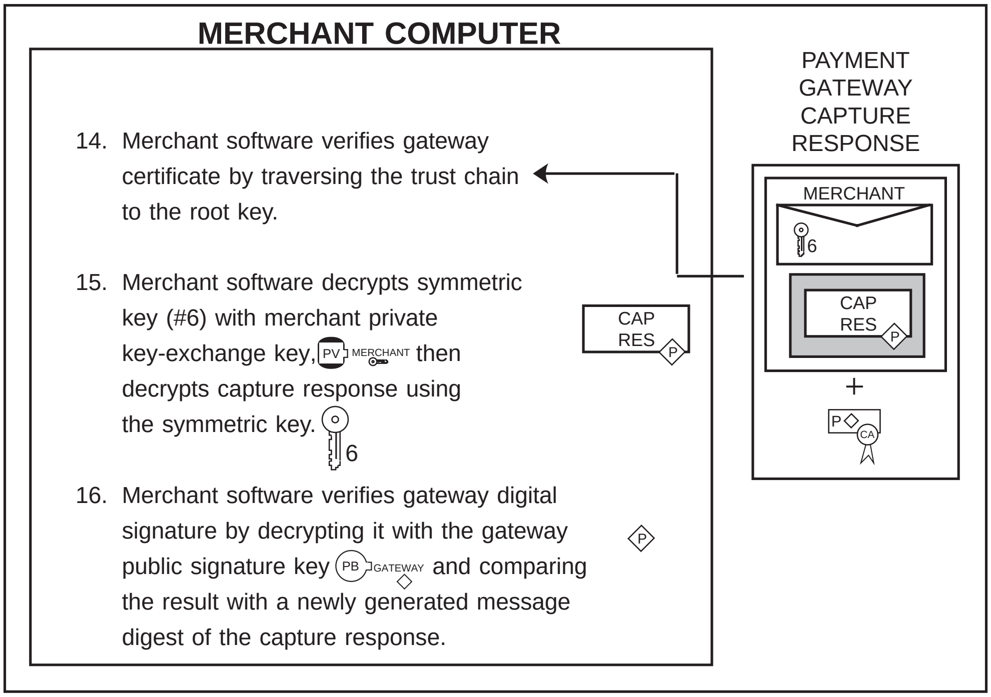
Continued on next page

4.6 Payment Capture, continued

When the merchant software receives the capture response message from the Payment Gateway, it decrypts the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypt the response message. It then verifies the Payment Gateway signature certificate by traversing the trust chain to the root key. It uses the Payment Gateway public signature key to check the Payment Gateway digital signature.

The merchant software stores the capture response to be used for reconciliation with payment received from the Acquirer.

Merchant receives response



14. Merchant software verifies gateway certificate by traversing the trust chain to the root key.

15. Merchant software decrypts symmetric key (#6) with merchant private key-exchange key, PV MERCHANT then decrypts capture response using the symmetric key. 6

16. Merchant software verifies gateway digital signature by decrypting it with the gateway public signature key PB GATEWAY and comparing the result with a newly generated message digest of the capture response.