Secure Electronic Transaction (SET) Specification

Book 1: Business Description

DRAFT for public comment
February 23, 1996

Macintosh

This document is a DRAFT intended to solicit public comment. It should not be used to build applications because there will be changes to the document after the review period. Readers can use this document to understand the intent of SET and are encouraged to provide feedback to facilitate the development of SET.

Readers are encouraged to comment on substantial issues. These specifications will continue to be reviewed and updated to ensure clarity and internal consistency.

MasterCard and Visa will create a process for applications to be certified as compliant with the SET specifications.

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.
- Associations 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 that will satisfy market demand is the development of a single, open industry specification.

Secure Electronic Transaction protocol

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

Advice and assistance in the development of these specifications have been provided by GTE, IBM, Microsoft, Netscape, SAIC, Terisa, and Verisign.

Contents

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

Audience

It is intended as an introduction to SET for anyone interested in the processing of bankcard transactions on electronic networks including by 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* below.)

Continued on next page

Preface, continued

Organization

Introduction	This section provides the background for understanding SET.
Business Requirements	This section introduces the business requirements that are addressed by the SET specification.
Concepts	This section offers background information on cryptography and certificate issuance.
Payment Processing	This section describes the most common SET transaction flows.
Acronyms and Glossary	This section defines terms and abbreviations used in the description of SET.

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

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.

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 Assymmetric 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 Date Security, Inc., Version 1.5, revised Nov. 1, 1993.

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

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 35
4.3 MERCHANT REGISTRATION 43
4.4 PURCHASE REQUEST 51
4.5 PAYMENT AUTHORIZATION 59
4.6 PAYMENT CAPTURE 64

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 bankcard purchases made through this medium will grow as Internet-based on-line 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 underway.

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 can display text, sound, images and even video, allowing merchants to transmit information directly to potential consumers around the world around the clock.

Consumer payment devices

With open networks, payments will increasingly be made 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, round-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 areas must be addressed to facilitate the future growth of bankcard transaction volume in the electronic marketplace.

Role of payment systems

Payment systems and their member financial institutions will play a significant role by establishing open specifications for bankcard payments 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 bankcard payments.

Use of bankcard products

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

Continued on next page

1.1 Background, continued

Purpose of Secure Electronic Transaction

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

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

These specifications will enable greater bankcard acceptance, with a level of security that will encourage consumers and business to make wide usage of bankcard products in this emerging market.

1.2 Objectives

Motivation

The primary motivation for the bankcard associations to provide specifications for secure payments are:

- to have the bankcard community take a leadership position in establishing a secure payment specifications and, in the process, avoid any cost associated with future reconciliation of implemented approaches,
- to respect and preserve the relationship between merchants and Acquirers and between cardholders and Issuers,
- to facilitate rapid development of the marketplace,
- to respond quickly to the needs of the financial services market, and
- to protect the integrity of bankcard brands.

Payment Security

The objectives of payment security are to:

- provide authentication of 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 one vendor will interoperate with applications developed by other vendors,
- create and support an open bankcard standard,
- define exportable technology throughout, in order 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 hardware and software platform 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 merchant, and cardholders and issuers,
- allow for minimum impact to existing merchant, acquirer and association applications and infrastructure, and
- provide an efficient protocol viewed from the financial institution perspective.

2 Business Requirements

2.1 Requirements

Introduction

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

Security issues

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

Seven business requirements

There are seven major business requirements addressed by SET:

1. Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information.
2. Ensure integrity for all transmitted data.
3. Provide authentication that a cardholder is a legitimate user of a branded bankcard account.
4. Provide authentication that a merchant can accept branded bankcard payments 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 of an electronic commerce transaction.
6. Ensure the creation of a protocol that is neither dependent on transport security mechanisms nor prevents their use.
7. Facilitate and encourage interoperability across software and network providers.

2.2 Features

Features of the specifications

These requirements are addressed by the following features of these specifications:

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

For the sake of clarity, each of these features has been described as a distinct component. It should be noted, however, that these elements do not function independently; all security functions must be implemented.

Confidentiality of information

To facilitate and encourage electronic commerce using bankcard products, it will be necessary to assure cardholders that their payment information is safe and accessible only 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.

On-line shopping: In today's on-line shopping environment, bankcard payment instructions are often transmitted from cardholders to merchants over open networks with little or no security precautions. However, this account information provides the key elements needed to create counterfeit cards 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 bankcard account numbers out of 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.

Confidentiality is ensured by the use of message encryption.

Continued on next page

2.2 Features, continued

Integrity of data

The specifications must guarantee that message content is not altered during the transmission between originator and 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. In order to eliminate this potential source of fraud and/or error, SET must provide the means to ensure that the contents of all order and payment messages received match the contents of messages sent.

Payment information integrity is ensured by the use of digital signatures.

Cardholder account authentication

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

These specifications define the mechanism to verify that a cardholder is a legitimate user of a valid bankcard account number.

Note: these specifications do not define the process whereby a financial institution determines if an individual is a legitimate user of an account.

Cardholder account authentication is ensured by the use of digital signatures and cardholder certificates.

Continued on next page

2.2 Features, continued

Merchant authentication

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

Merchant authentication is ensured by the use of digital signatures and merchant certificates.

Interoperability

The specifications must be applicable on a variety of hardware and software platforms and must include no 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.

Interoperability is ensured by the use of specific protocols and message formats.

2.3 Scope

Use of bankcards

The SET specifications address 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 bankcards.

Electronic shopping experience

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

Stage	Description
1	The cardholder browses for items. This may be accomplished in a variety of ways, such as: • using a browser to view an on-line 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 a 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 on-line 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. These specifications focus on the case when a bankcard is selected.
5	The cardholder sends the merchant a completed order along with a means of payment. In these specifications, 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

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.

Even though these steps have been described as occurring in a specific order, variations are possible; many such variations are described later in these specifications.

These specifications focus on steps 5, 6, 7 and 9 when the cardholder chooses to use a bankcard as the means of payment.

Within the scope

The following are within the scope of these specifications:

- 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 these specifications:

- 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 bankcards

Note: this list illustrates categories of things that are outside the scope of the SET specifications; it is not intended to be complete.

3 Concepts

3.1 Payment System Participants

Interaction of participants

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

Cardholder

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

Issuer

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

Merchant

A merchant offers goods for sale or provides services in exchange for payment. SET allows a merchant to offer electronic interactions that cardholders can use securely. A merchant that accepts bankcards for payment must have a relationship with an Acquirer.

Acquirer

An Acquirer is the financial institution that establishes an account with a merchant and processes bankcard 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

Association

Financial institutions have founded bankcard associations that protect and advertise the brand, establish and enforce rules for use and acceptance of bankcards, and provide networks to interconnect the financial institutions.

Third Parties

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

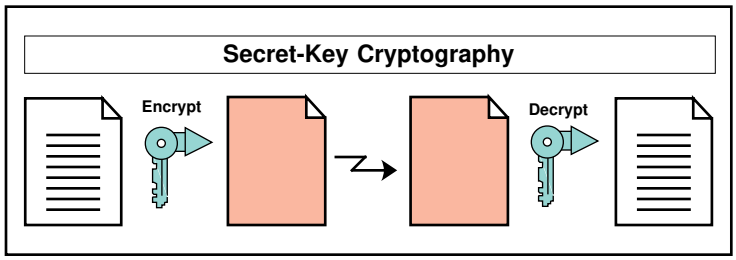
3.2 Cryptography

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 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.

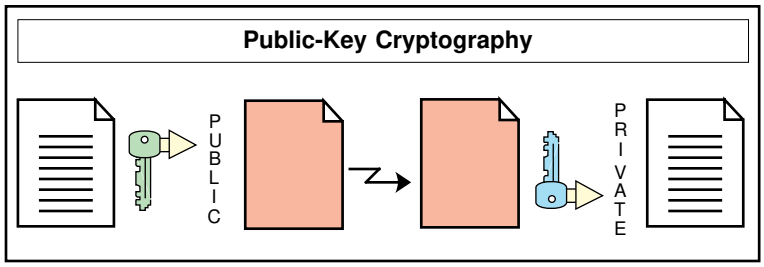


Continued on next page

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 such 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 by the user using the private key. *This assurance is only maintained if the user ensures that the private key is not disclosed to another.* 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).



Secret-key cryptography is impractical for exchanging messages with a large group of previously unknown correspondents over a public network. In order for a merchant to conduct transactions securely with millions of Internet subscribers, each consumer would need a distinct key assigned by the 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 the merchant.

Continued on next page

3.2 Cryptography, continued

Encryption

Confidentiality is ensured by the use of message encryption.

Encryption: relationship of keys

When two users want to exchange messages securely, each 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, the public keys can be transmitted over an insecure network without fear that an eavesdropper can 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.

Encryption: use of symmetric key

SET will rely on cryptography to ensure message confidentiality. In SET, message data will initially 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 such 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.

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.

Digital signatures: 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, i.e., 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 on average change half of the bits in the message digest. Roughly, the odds of two messages having the same message digest are one in 1,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000. It is computationally infeasible to generate two different messages that have the same message digest.

3.2 Cryptography, continued

Digital signatures: example

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.

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.

Certificates: need for 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

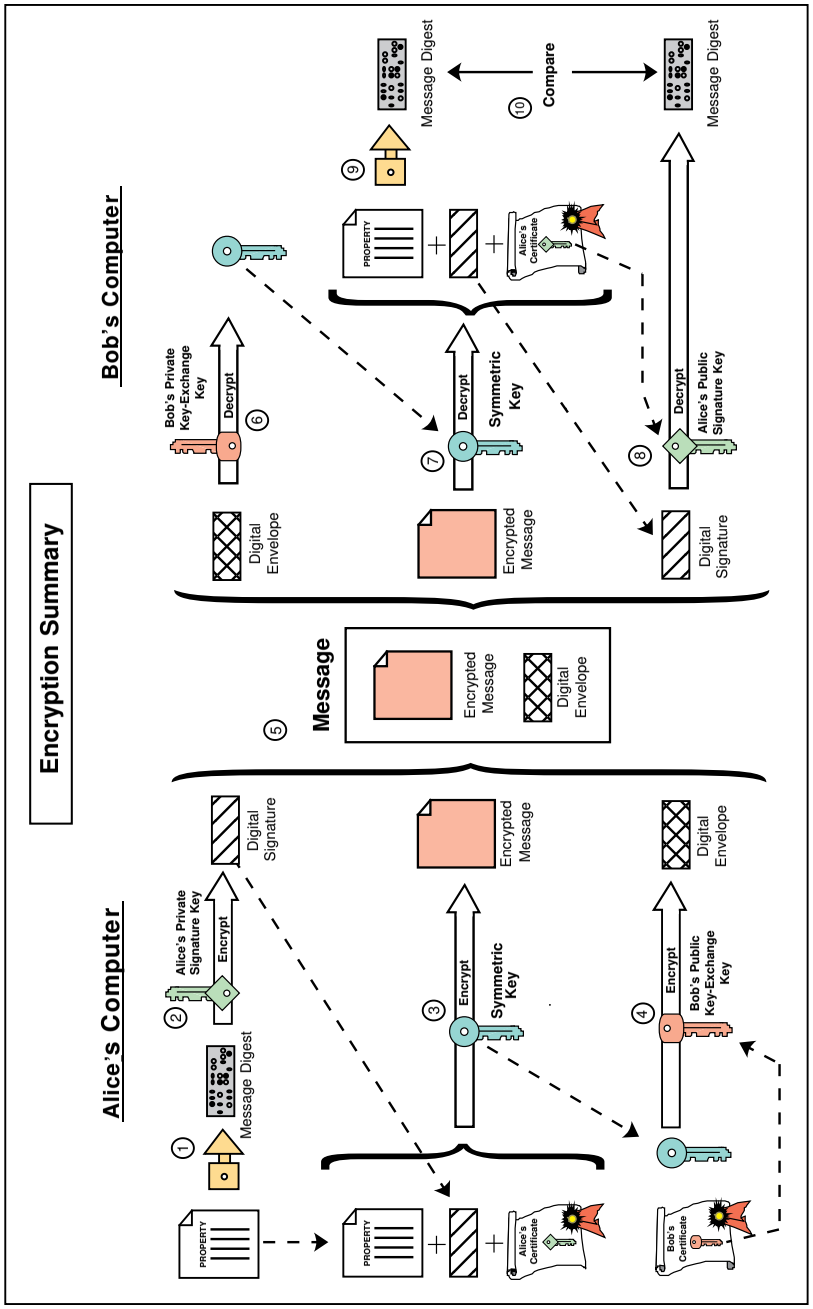
The means that a financial institution uses to authenticate a cardholder or merchant is not defined by these specifications. Each bankcard association and financial institution will select an appropriate method.

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 a property description and send it in an encrypted message to Bob. The numbered steps in the diagram are explained on the following pages.



Continued on next page

3.2 Cryptography, continued

Encryption

The encryption process of the diagram on the previous page 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. In order 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, is sent to Bob along with the encrypted message itself.
5	Finally, she 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).

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.

Continued on next page

3.2 Cryptography, continued

Step	Action
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

Introduction of 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.

Generation of 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 bankcard. Because they are digitally signed by a financial institution, they cannot be altered by a third party and only the financial institution can generate one. The certificates contain the account number and expiration date, which are encoded using a one-way hashing algorithm. If the account number and expiration date 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 to the payment gateway where the link is verified.

These certificates are only issued to the cardholder upon approval of the cardholder's issuing financial institution. By requesting a certificate, a cardholder has indicated the intent to perform commerce via electronic means. These certificates are transmitted to merchants with purchase requests and encrypted payment instructions. Upon receipt of the cardholder's certificates, 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 these specifications, cardholder certificates are optional at the bankcard association'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 bankcard brand.) Because they are digitally signed by the merchant's financial institution, they cannot be altered by a third party and only the financial institution can generate one.

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 in order 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 bankcard 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 accept and process certificate requests initiated by merchants. Acquirers receive their certificates from each bankcard association.

Issuer certificates

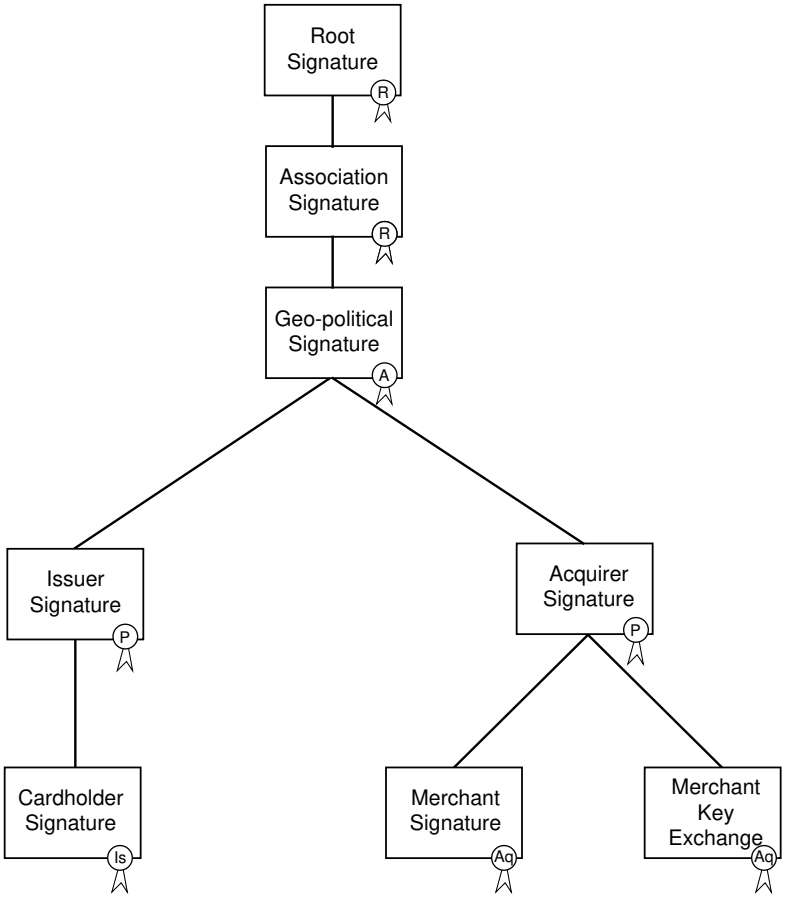
An Issuer must have certificates in order operate a Certificate Authority that can accept and process certificate requests directly from cardholders over public and private networks. Those Issuers that choose to have the bankcard association process certificate requests on their behalf will not require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

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 Association on behalf of the Issuer). The Issuer's certificate is linked back to a root key through the Association'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. This hierarchy is illustrated by the following diagram.



The number of levels shown in this diagram is illustrative. A bankcard association may not always operate a geo-political CA 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 be generated. This 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

There are many ways that cardholders will shop. This section describes two ways. The SET protocol supports each of these shopping experiences and should support others as they are defined.

On-line catalogues

The growth of electronic commerce can largely be attributed to the popularity of the World Wide Web. Merchants can tap into this popularity by creating virtual storefronts on the Web that contain on-line catalogues. These catalogues can be quickly updated as merchant's product offerings change or to reflect seasonal promotions.

Cardholders can visit these Web pages selecting items for inclusion on an order. Once the cardholder finishes shopping, the merchant's Web server can send a completed order form for the cardholder to review and approve.

Once the cardholder approves the order and chooses to use a bankcard for payment, the SET protocol provides the mechanisms for the cardholder to securely transmit payment instructions as well as for the merchant to obtain authorization and receive payment for the order.

Electronic catalogues

Merchants may distribute catalogues on electronic media such as diskettes 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 bankcard for payment, 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

Transactions described

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

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

- Cardholder registration
- Merchant registration
- Purchase request
- Payment authorization
- Payment capture

Other transactions

The following additional transactions are part of these specifications, but are not described in this section:

- Certificate query
- Purchase inquiry
- Purchase notification
- Sale transaction
- Authorization reversal
- Capture reversal
- Credit
- Credit reversal

A Guide to the Diagrams

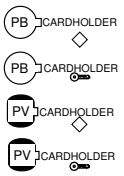
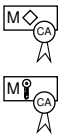
The table below may be used as a reference for identifying the participant who digitally signed a message or certificate in the detailed diagrams of this section.

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

Continued on next page

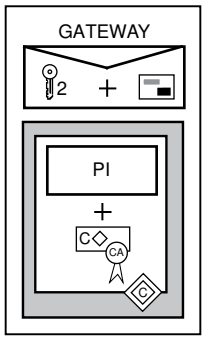
4.1 Overview, continued

The following symbols are used in the detailed diagrams in this section:

	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. Also, 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.
	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 bankcard and is used to indicate when the cardholder's account number is being transmitted in the digital envelope along with the symmetric encryption key.

Continued on next page

4.1 Overview, continued

	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.

Note: The **bold text** in the detailed diagrams of this section 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 (i.e. either the software displays an acknowledgment message or the user must perform a trivial action like clicking an icon).

Protocol Description

In the event that the description of the processing in this section differs from the Technical Specifications, the Technical Specifications take precedence.

Continued on next page

4.1 Overview, continued

Certificate Authority Functions

The diagrams and processing flows that follow describe the functions 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 in reality they may be performed by one to three entities. Bankcard associations 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 presents some suggestions for some *possible* arrangements with variations on distribution:

- A company that issues proprietary cards performs all three steps for its cardholders.
- A financial institution receives, processes and approves certificate requests for its cardholders or merchants and forwards the information to the appropriate bankcard association(s) to issue the certificates.
- Certificate requests are received by an independent *Registration Authority* that processes bankcard certificate applications for multiple bankcard brands and forwards requests to the appropriate financial institution (Issuer or Acquirer) for processing; the financial institution forwards approved requests to the bankcard association to issue the certificates.

These scenarios are simply suggestions of some possible arrangements. Bankcard associations 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 bankcard brand. Bankcard associations at their option may allow cardholders to process transactions without a certificate as a temporary measure to facilitate implementation of these specifications.

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.

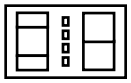
Strength of cardholder certificates

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 employed by the bankcard association and the bankcard issuer to authenticate the cardholder prior to the bankcard being issued.

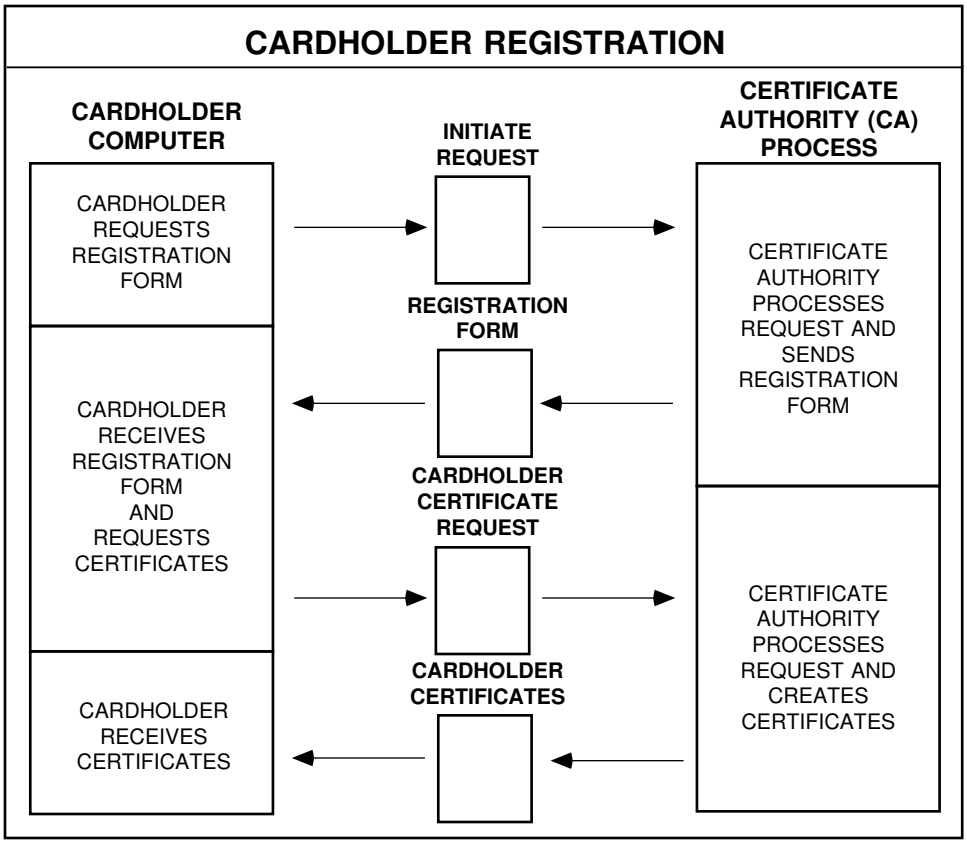
Cardholder authentication

The SET protocol uses a cardholder signature certificate to confirm that a transaction is from a registered user of a bankcard. If a cardholder signature certificate is not present, authentication of the cardholder must be performed by other means.

4.2 Cardholder Registration

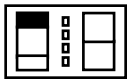


The figure shown below provides a high level overview of the cardholder registration process. This scenario is divided into its five fundamental steps in the following detailed sections. The icon to the left corresponds to the diagram below and serves as a map to this scenario; it is repeated in the explanations of the more detailed diagrams with a shaded region that indicates which step is being described.



Continued on next page

4.2 Cardholder Registration, continued

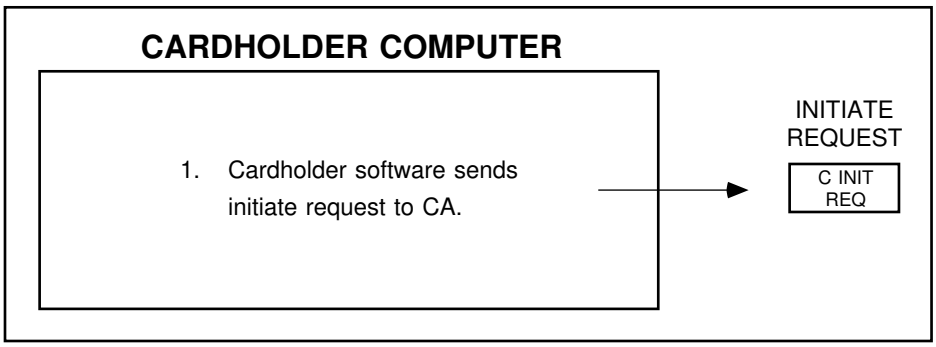


Cardholders must register with a Certificate Authority (CA) before they can send SET messages to merchants. In order to send SET messages to the CA, the cardholder must have a copy of the CA public key-exchange key, which is provided in the CA key-exchange certificate.

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

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

Cardholder Requests Registration Form

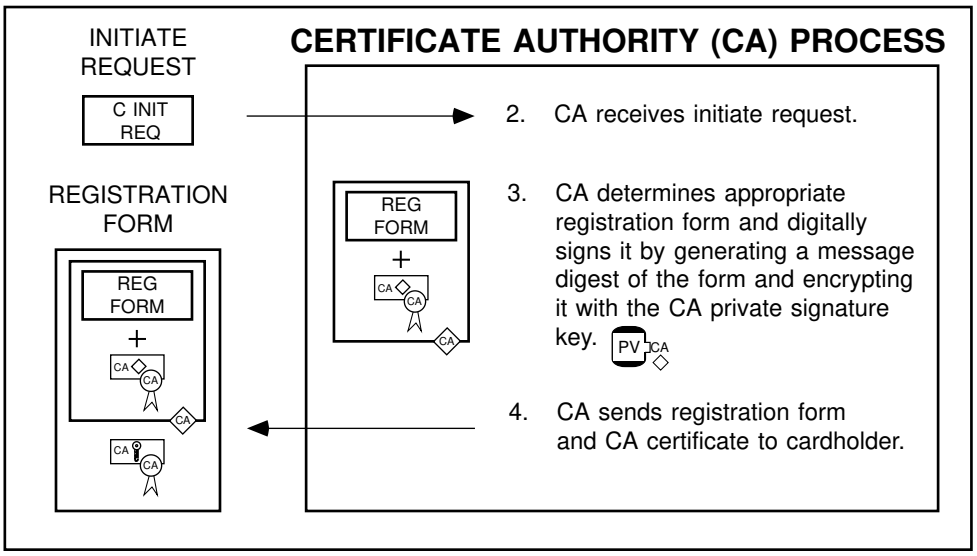


Continued on next page

4.2 Cardholder Registration, continued

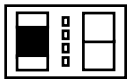
The CA identifies the cardholder's financial institution (using the first six digits of the account number) and selects the appropriate registration form. It returns this registration form along with a copy of its own key-exchange certificate to the cardholder.

Certificate Authority Processes Request and Sends Registration Form



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 software must hold the CA certificate to use later during the registration process. Once the software has a copy of the CA key-exchange certificate, the cardholder can register an account for use with SET.

The cardholder needs two public/private key pairs for use with SET: key-exchange and signature. The cardholder software generates these key pairs if they do not already exist. Note: the key-exchange key is only used during the certificate processing and no key-exchange certificate is issued.

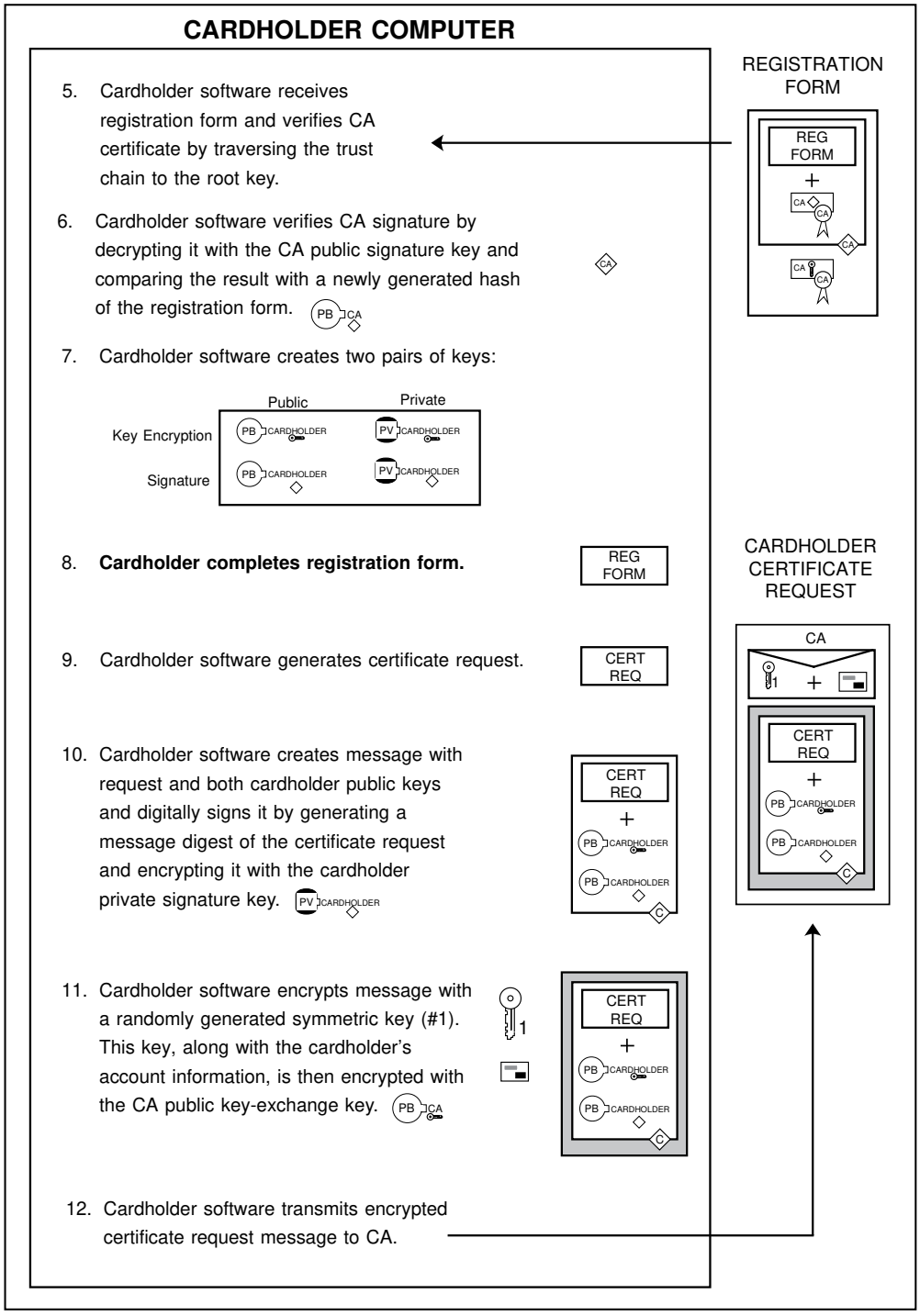
To register an account, the cardholder fills out the registration form that was returned by the CA with information such as the cardholder's name, account number, expiration date, account billing address, and any additional information the issuing financial institution deems necessary to identify the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

The cardholder software 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 registration 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.

Continued on next page

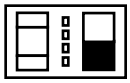
4.2 Cardholder Registration, continued

Cardholder Receives Registration Form and Requests Certificate



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 and the account number. 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.

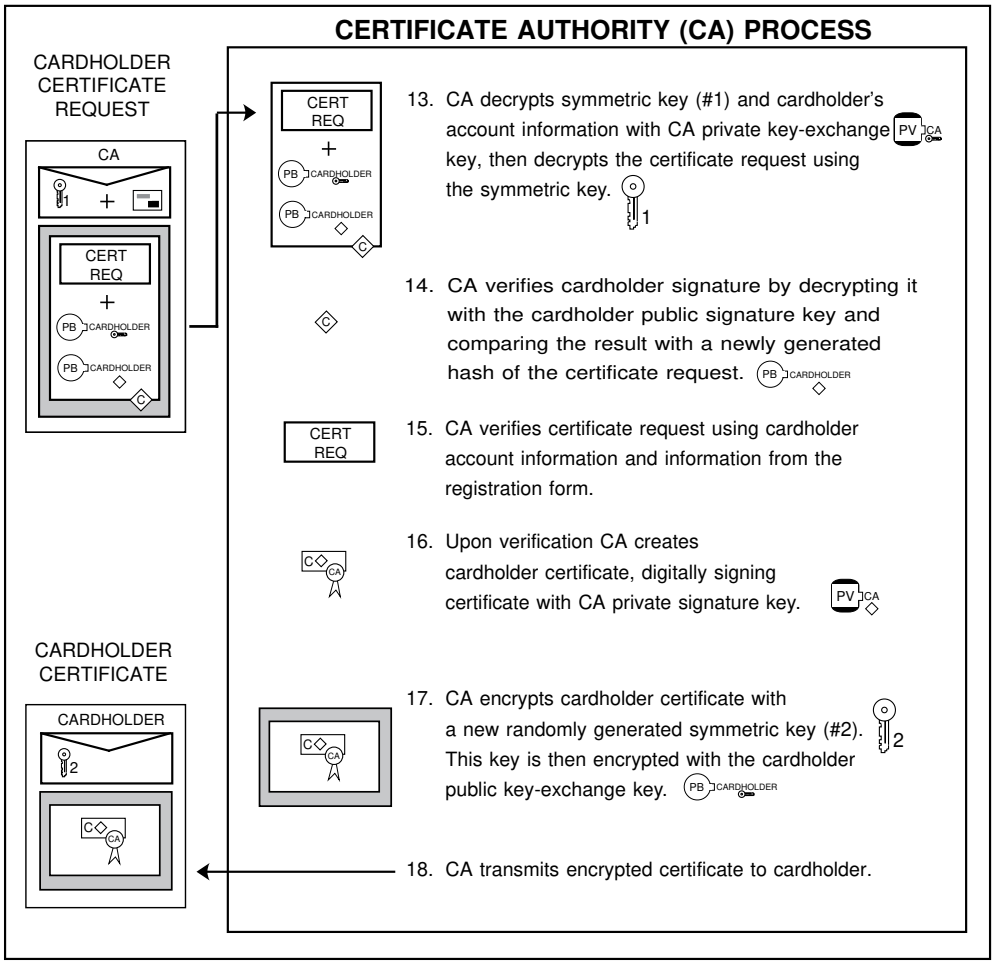
Next the CA must verify the information from the registration request using the cardholder's account information. The process by which the CA and the Issuer exchange information and the steps taken to verify the information in the registration request are outside the scope of these specifications. As described in Section 4.1, there are several ways to configure the processing performed by the CA and the Issuer, such as having the bankcard association 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, 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 bankcard, but it may expire sooner. The certificate is then encrypted using a new randomly generated symmetric key, which in turn is encrypted using the cardholder public key-exchange key. The response is then transmitted to the cardholder.

Continued on next page

4.2 Cardholder Registration, continued

Certificate Authority Processes Request and Creates Certificates



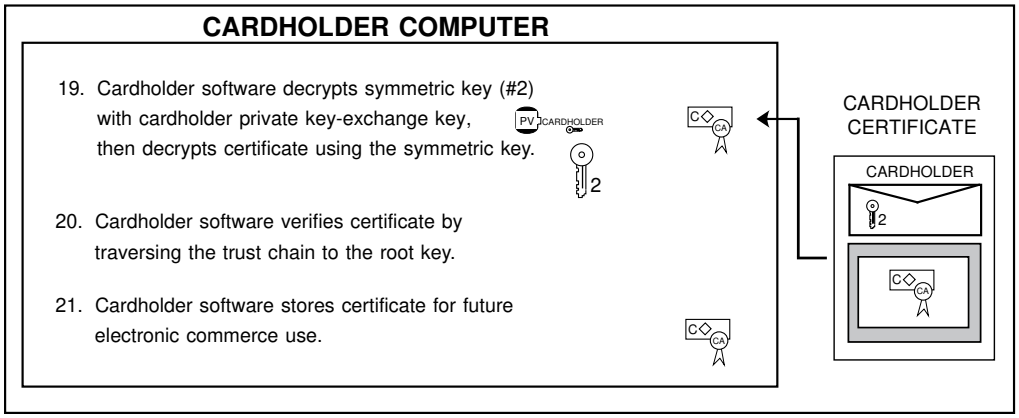
Continued on next page

4.2 Cardholder Registration, continued

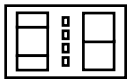
When the cardholder software receives the response from the CA, it decrypts the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypt the registration response containing the cardholder certificate.

After the cardholder software verifies the certificate by traversing the trust chain to the root key, it stores the certificate on the cardholder's computer for use in future electronic commerce transactions. Cardholder software vendors will ensure that the certificate and related information is stored in a way to prevent unauthorized access.

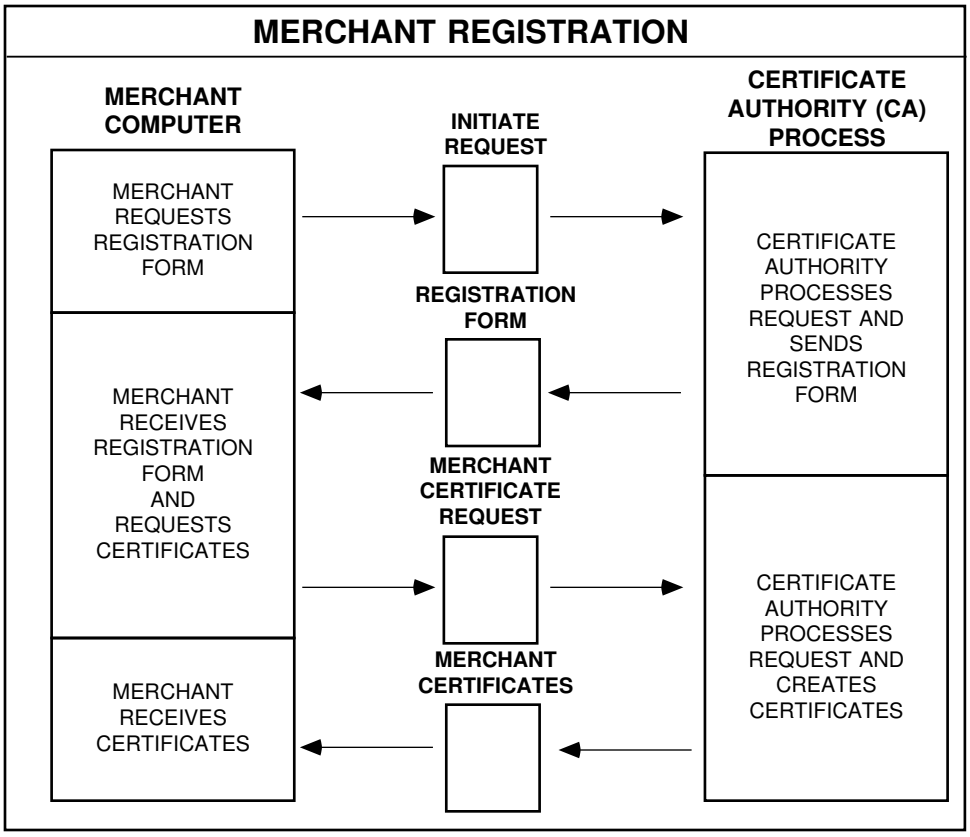
Cardholder Receives Certificates



4.3 Merchant Registration

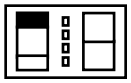


The figure shown below provides a high level overview of the merchant registration process. This scenario is divided into its five fundamental steps in the following detailed sections. The icon to the left corresponds to the diagram below and serves as a map to this scenario; it is repeated in the explanations of the more detailed diagrams with a shaded region that indicates which step is being described.



Continued on next page

4.3 Merchant Registration, continued

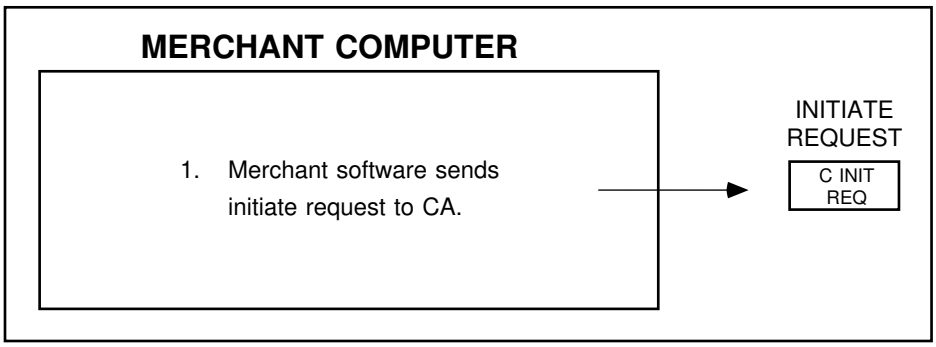


Merchants must register with a Certificate Authority (CA) before they can receive SET payment instructions from cardholders or process SET transactions through a payment gateway. In order to send SET messages to the CA, the merchant must have a copy of the CA public key-exchange key, which is provided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

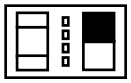
The registration process is started when the merchant software requests a copy of the CA's key-exchange certificate and the appropriate registration form.

Merchant Requests Registration Form



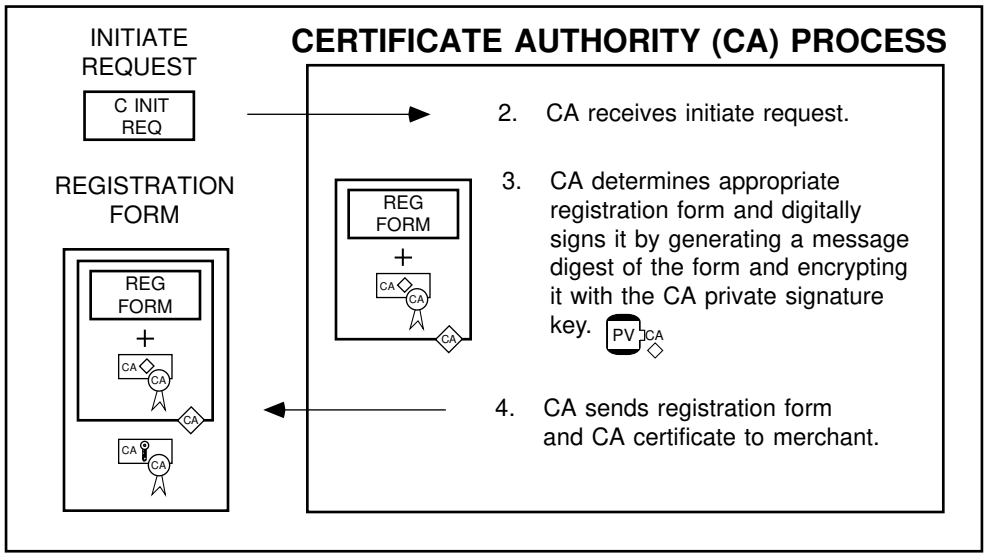
Continued on next page

4.3 Merchant Registration, continued



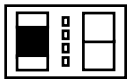
The CA identifies the merchant's financial institution and selects the appropriate registration form. It returns this registration form along with a copy of its own key-exchange certificate to the merchant.

Certificate Authority Processes Request and Sends Registration Form



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. The merchant software must hold 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.

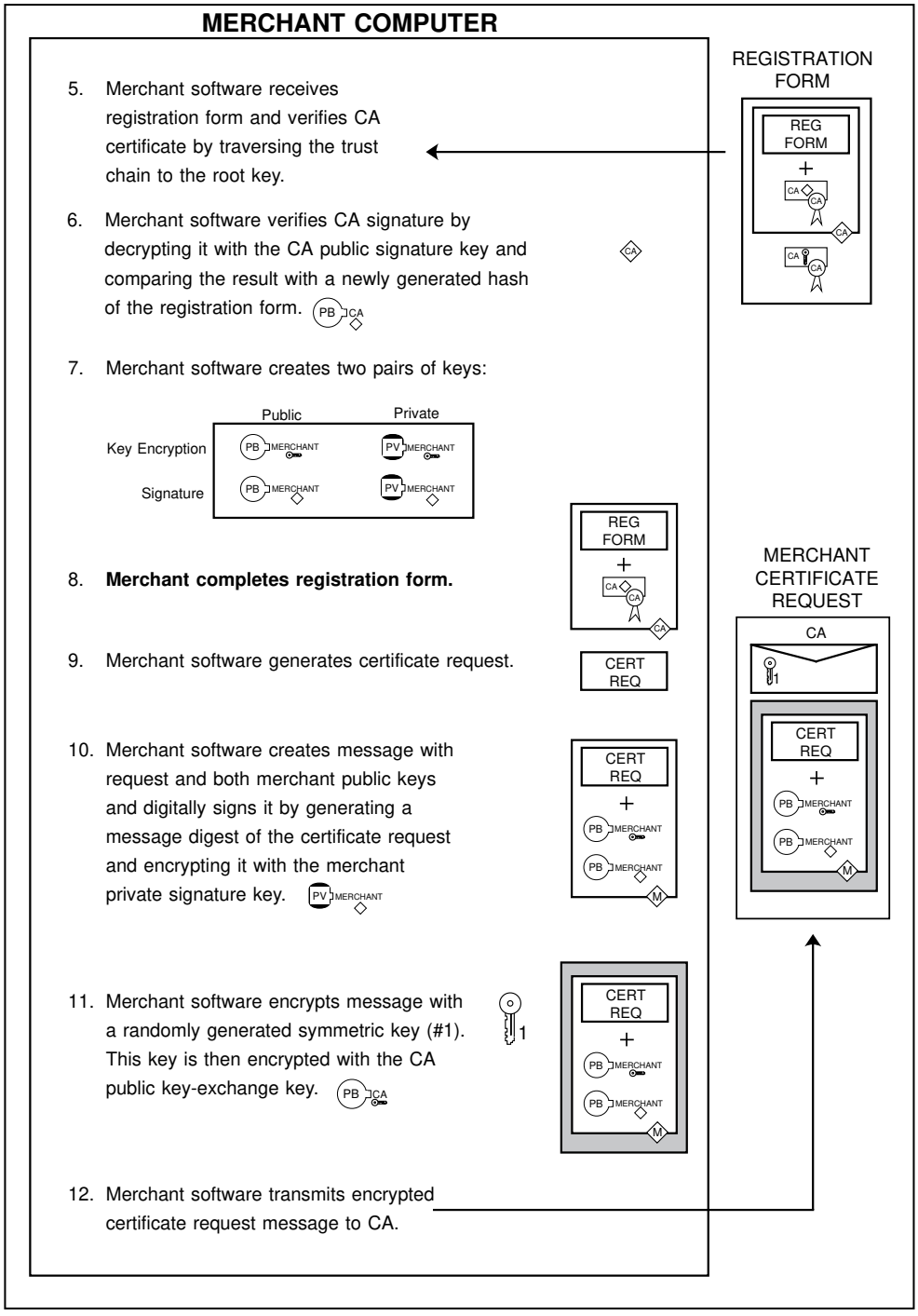
To register, the merchant fills out the registration form on the screen with information such as the merchant's name, address, and merchant ID.

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

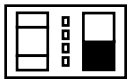
4.3 Merchant Registration, continued

Merchant Receives Registration Form and Requests Certificates



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 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.

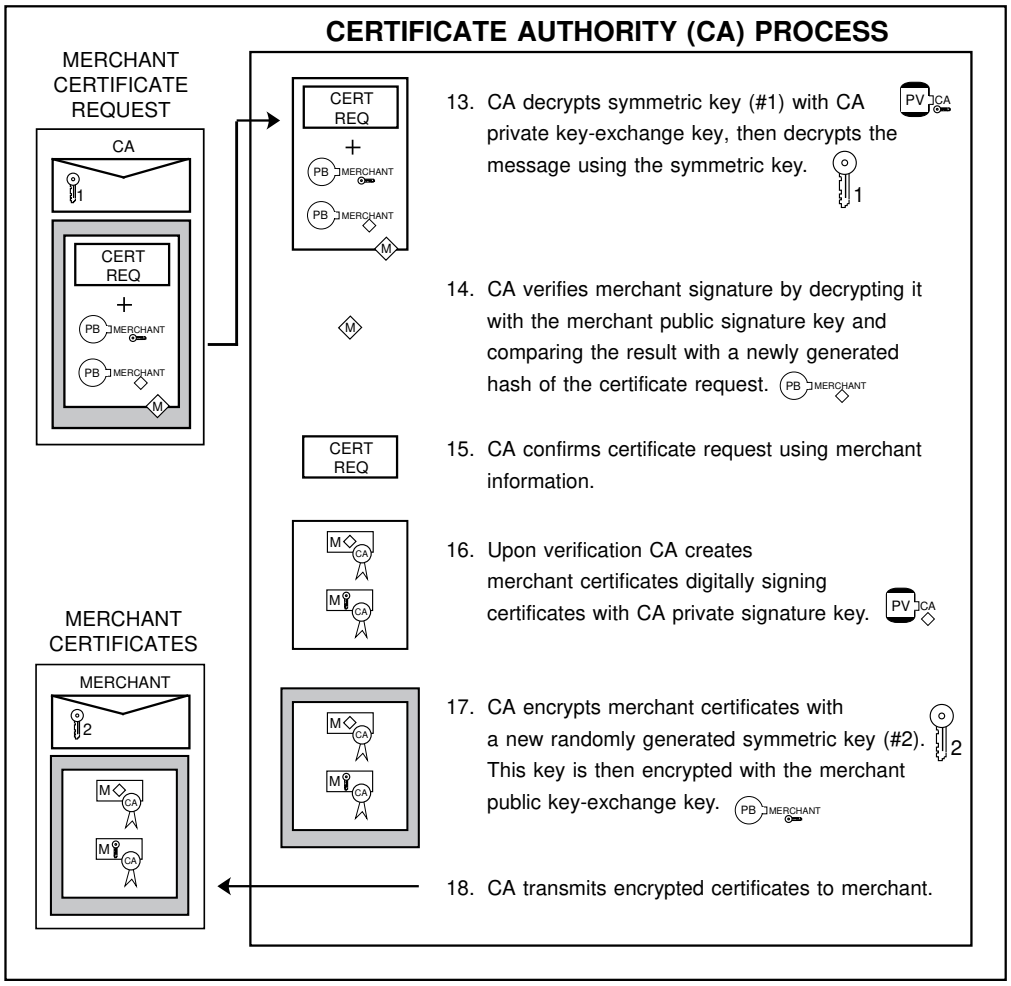
Next the CA must verify the information from the registration request using known merchant information. The process by which the CA and the Acquirer exchange information and the steps taken to verify the information in the registration request are outside the scope of these specifications. As described in Section 4.1, there are several ways to configure the processing performed by the CA and the Acquirer, such as having the bankcard association 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

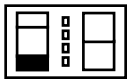
4.3 Merchant Registration, continued

Certificate Authority Processes Request and Creates Certificates



Continued on next page

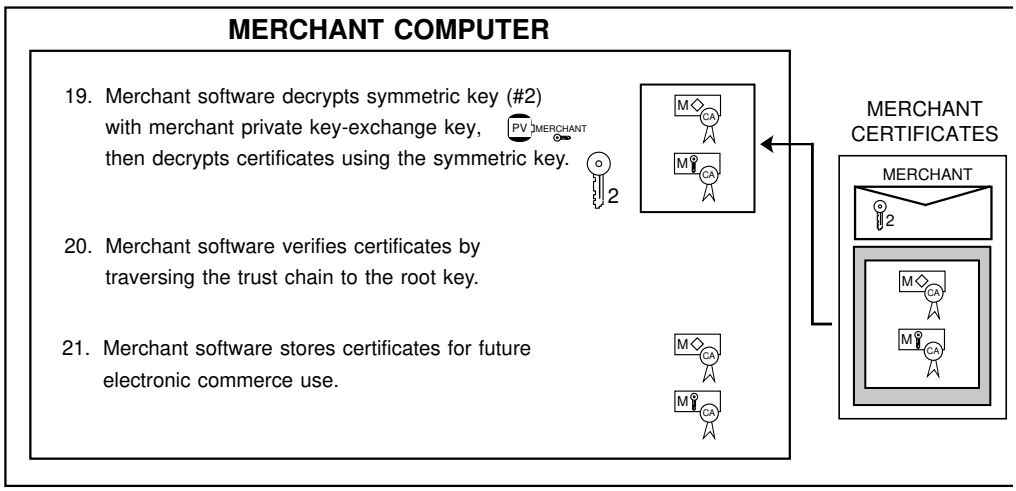
4.3 Merchant Registration, continued



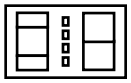
When the merchant software receives the response from the CA, it decrypts the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypt the registration response containing the merchant certificates.

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.

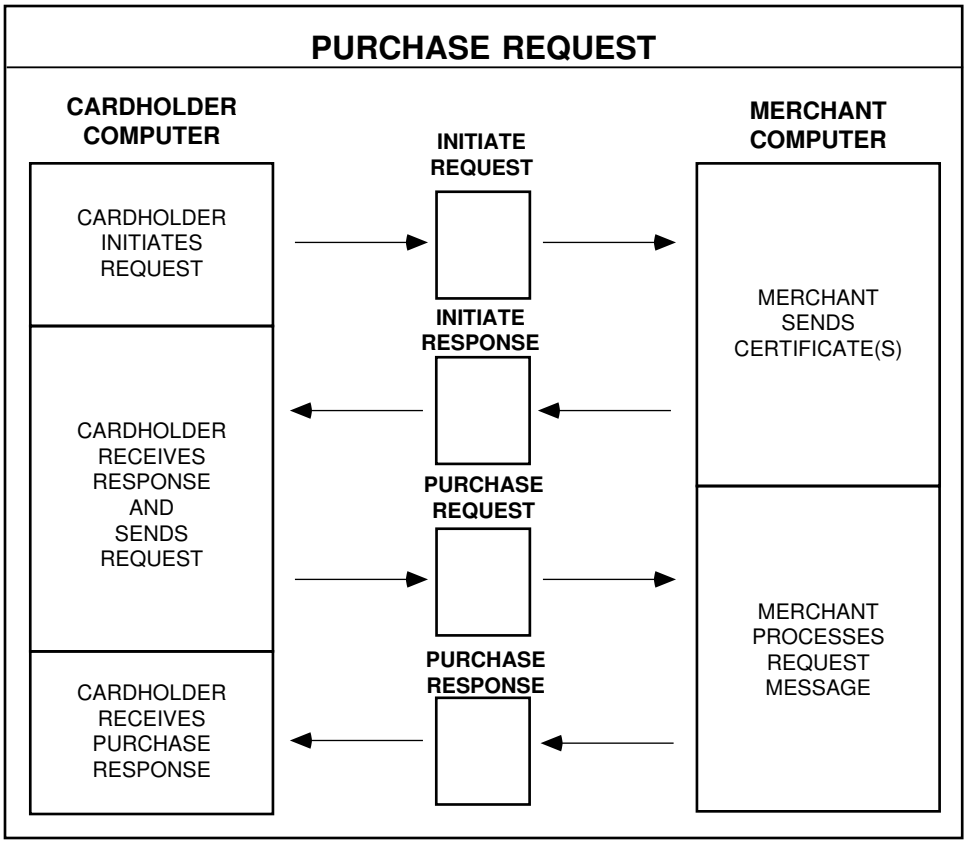
Merchant Receives Certificates



4.4 Purchase Request

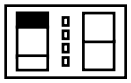


The figure shown below provides a high level overview of the purchase request portion of a cardholder's order process. This scenario is divided into its five fundamental steps in the following detailed sections The icon to the left corresponds to the diagram below and serves as a map to this scenario; it is repeated in the explanations of the more detailed diagrams with a shaded region that indicates which step is being described.



Continued on next page

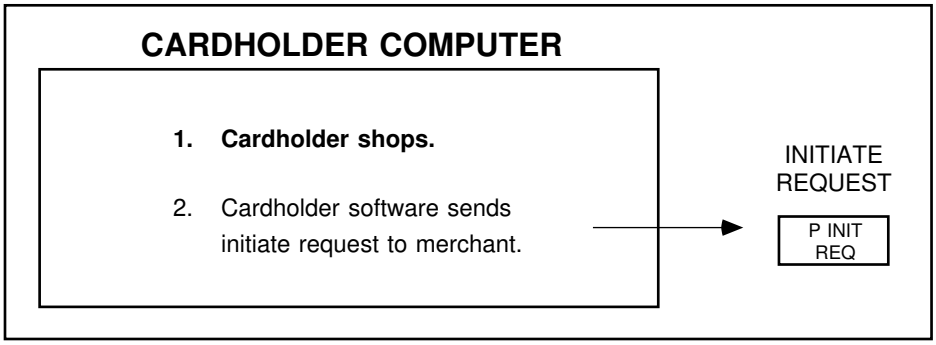
4.4 Purchase Request, continued



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. In addition, the cardholder will have selected a bankcard as the means of payment.

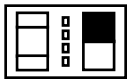
In order to send SET messages to a merchant, the cardholder must have a copy of the merchant public key-exchange key as well as the Payment Gateway's key-exchange keys. The SET order process is started when the cardholder requests a copy of the merchant's and gateway's certificates. The message from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

Cardholder Initiates Request



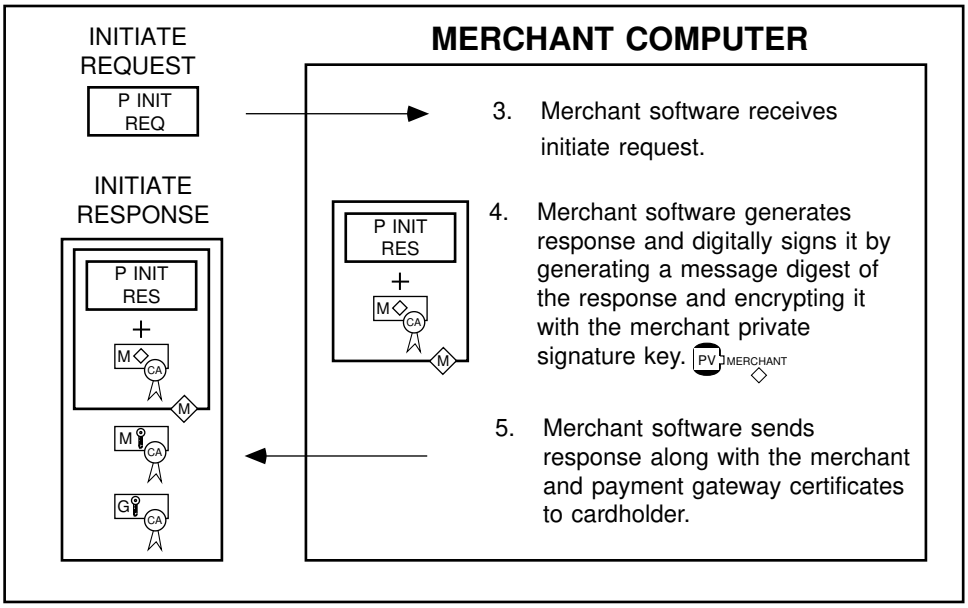
Continued on next page

4.4 Purchase Request, continued



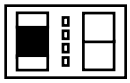
When the merchant receives the request, it assigns a unique transaction identifier to the message. It then transmits the merchant and gateway certificates that correspond to the bankcard brand indicated by the cardholder along with the transaction identifier to the cardholder.

Merchant Sends Certificate(s)



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. The software must hold these certificates to use later during the ordering process.

The cardholder software creates the Order Information (OI) and Payment Instructions (PI). The software includes the cardholder signature certificate with the OI; it also includes the cardholder signature certificate with the 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.

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.

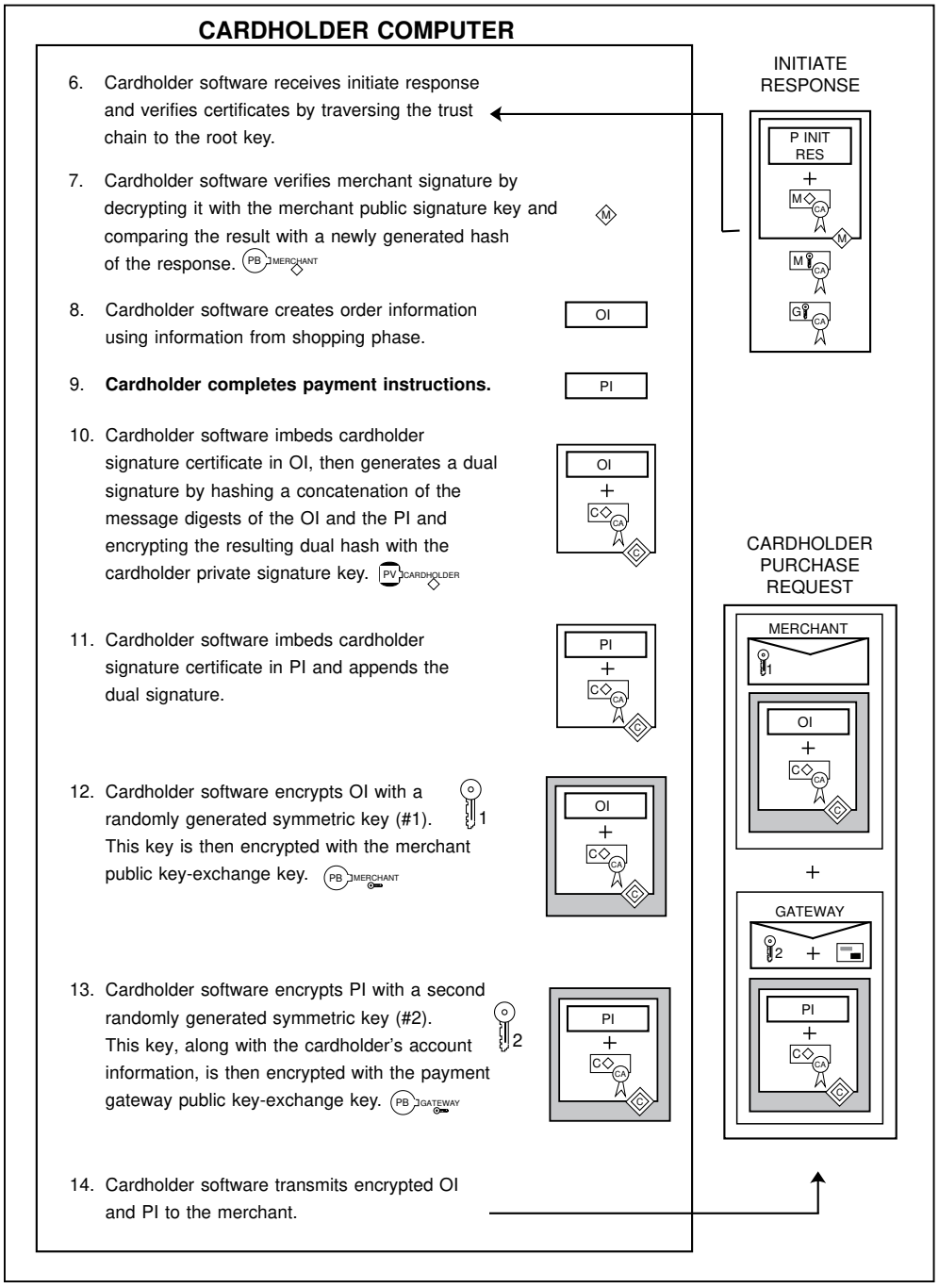
Next the software generates a random symmetric encryption key and uses it to encrypt the dual signed PI. The software then encrypts the cardholder account number as well as the random symmetric key used to encrypt the PI into a digital envelope using the Payment Gateway's key-exchange key.

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

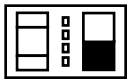
Cardholder Receives Response and Sends Request



Erratum: the OI is not encrypted as described in step 12 above.

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: Technical Specifications.)

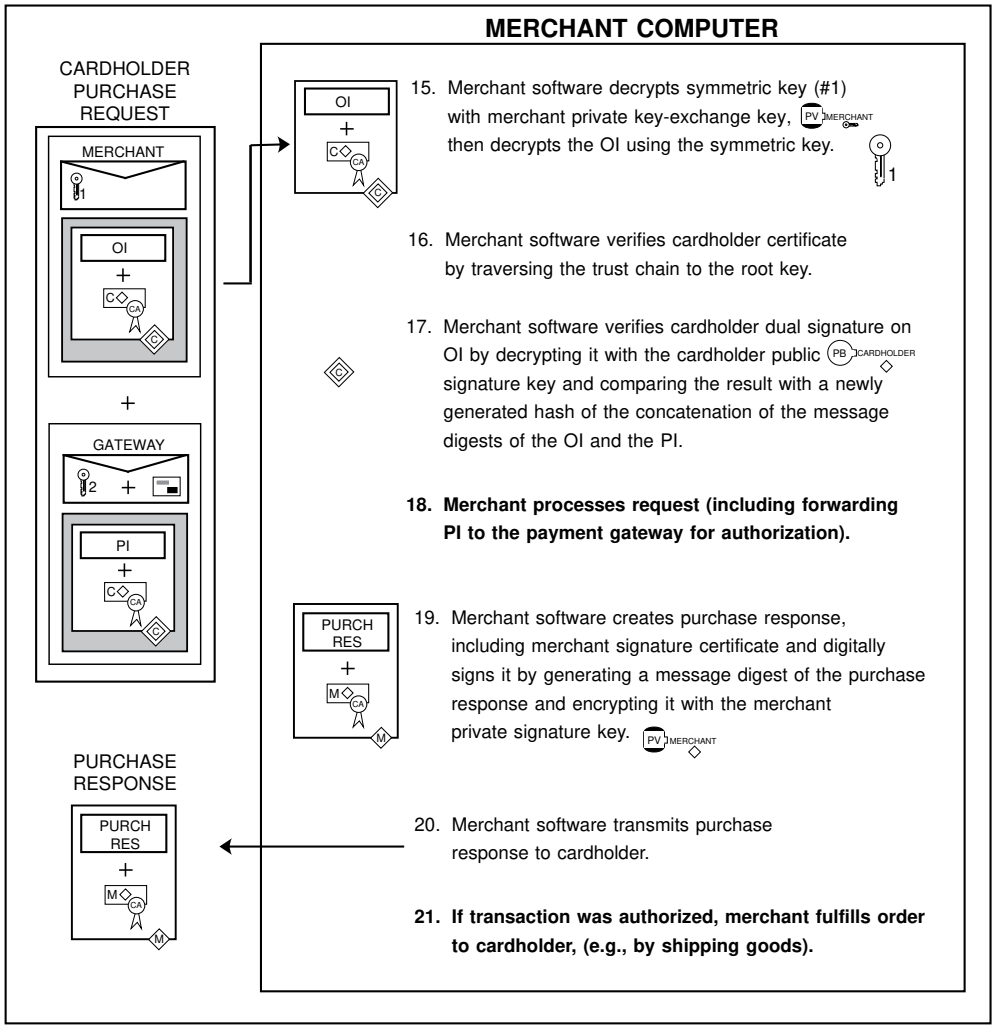
After the OI has been processed, the merchant software generates and digitally signs a purchase response message, which includes the merchant signature certificate and indicates that the cardholder's order has been received by the merchant. The response is then transmitted to the cardholder.

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



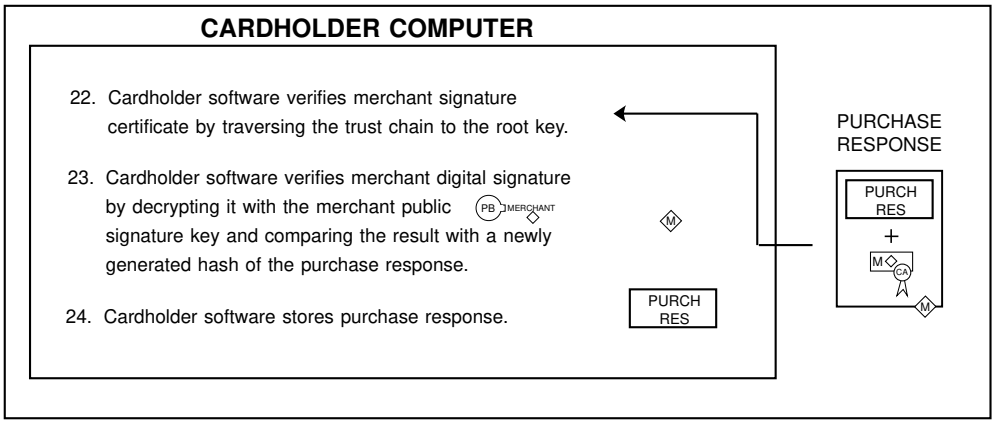
Erratum: the OI is not encrypted and therefore the decryption described in step 15 above does not occur.

Continued on next page

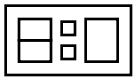
4.4 Purchase Request, continued

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.

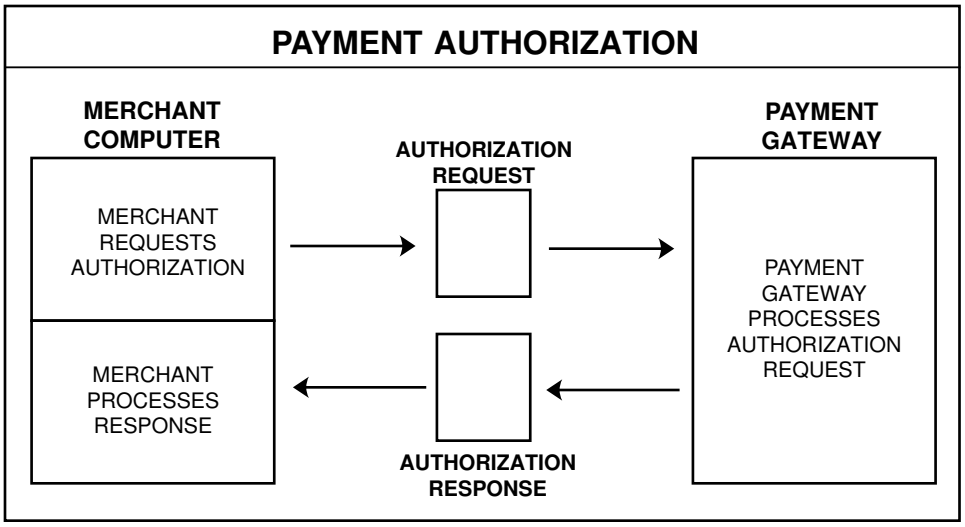
Cardholder Receives Purchase Response



4.5 Payment Authorization



The figure shown below provides a high level overview of a merchant's payment authorization process. This scenario is divided into its three fundamental steps in the following detailed sections The icon to the left corresponds to the diagram below and serves as a map to this scenario; it is repeated in the explanations of the more detailed diagrams with a shaded region that indicates which step is being described.



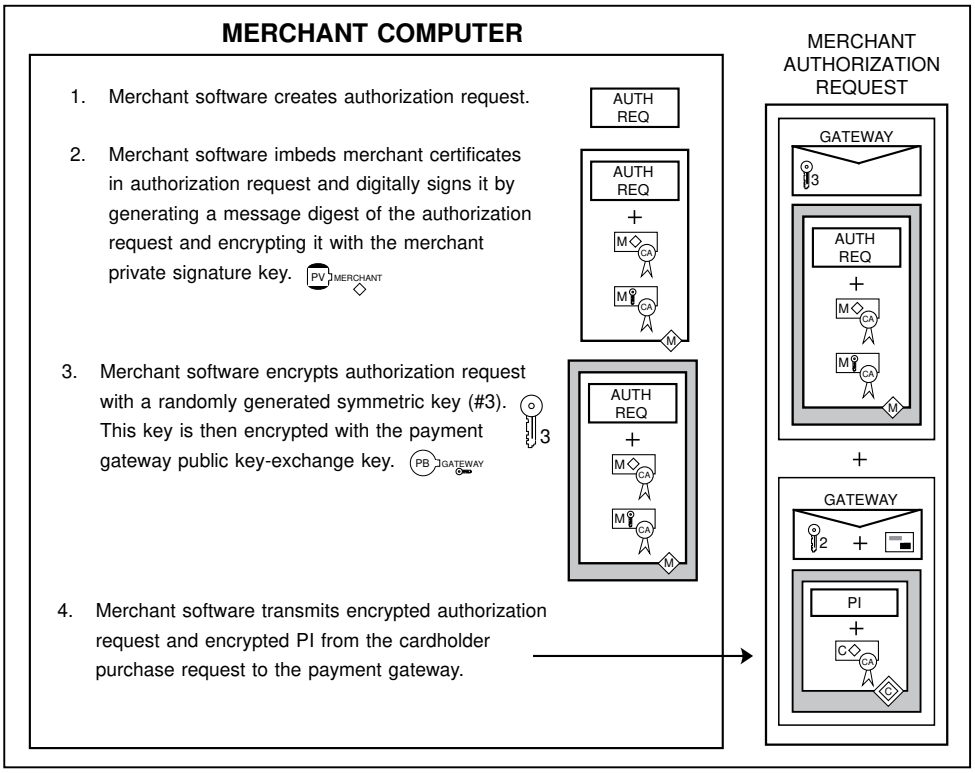
Continued on next page

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.

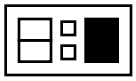
Note: the SET protocol also includes a sales transaction that allows a merchant to authorize a transaction and request payment in a single message. While the sales message includes an additional block of data on the request from the merchant, it otherwise parallels the message flow being described in this section.

Merchant Requests Authorization



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 bankcard payment system.

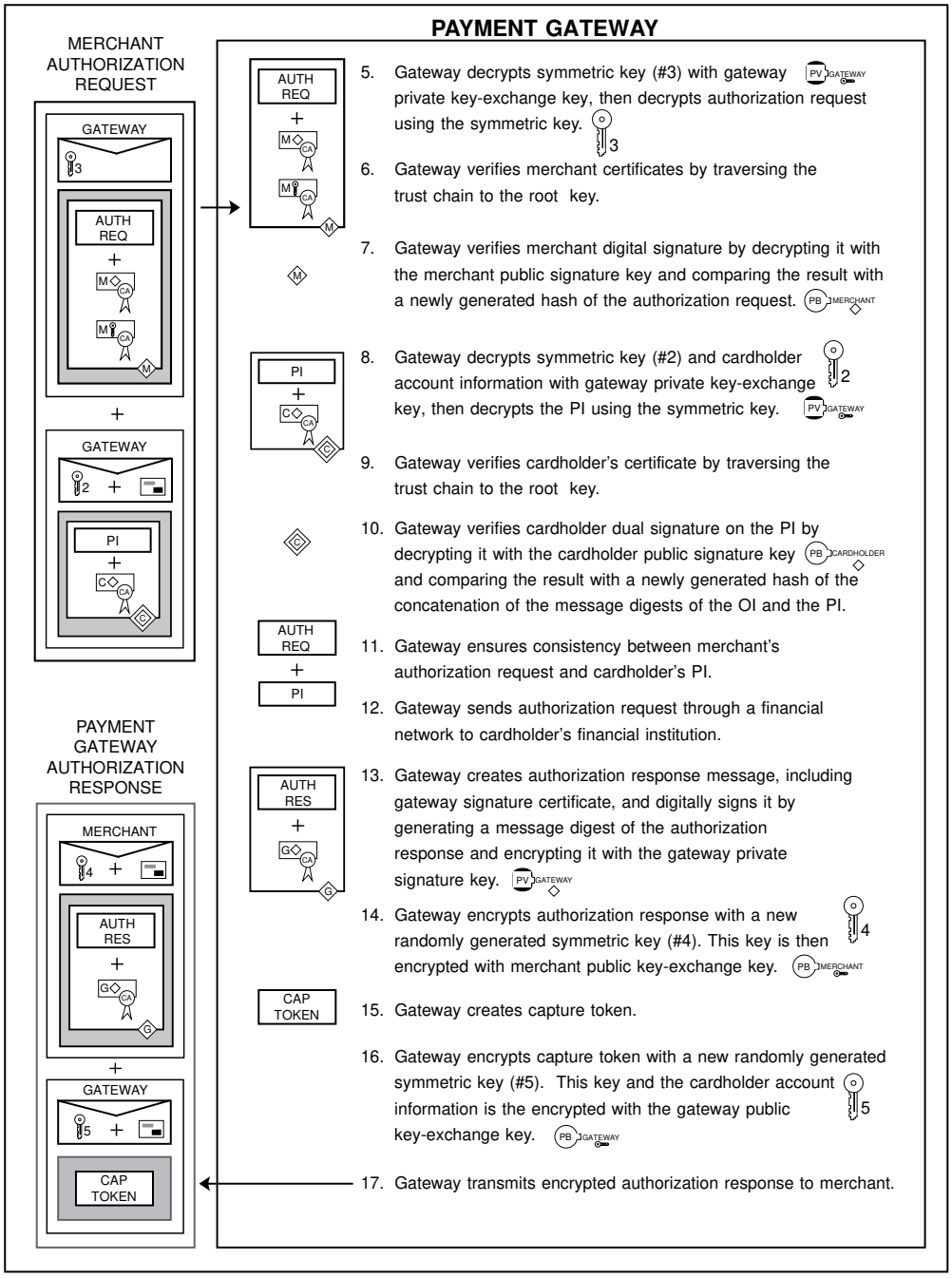
Upon receiving an authorization response from the Issuer, the Payment Gateway generates and digitally signs an authorization response message, which includes the Issuer's response and a copy of the Payment Gateway signature certificate. The response also includes an optional capture token with information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



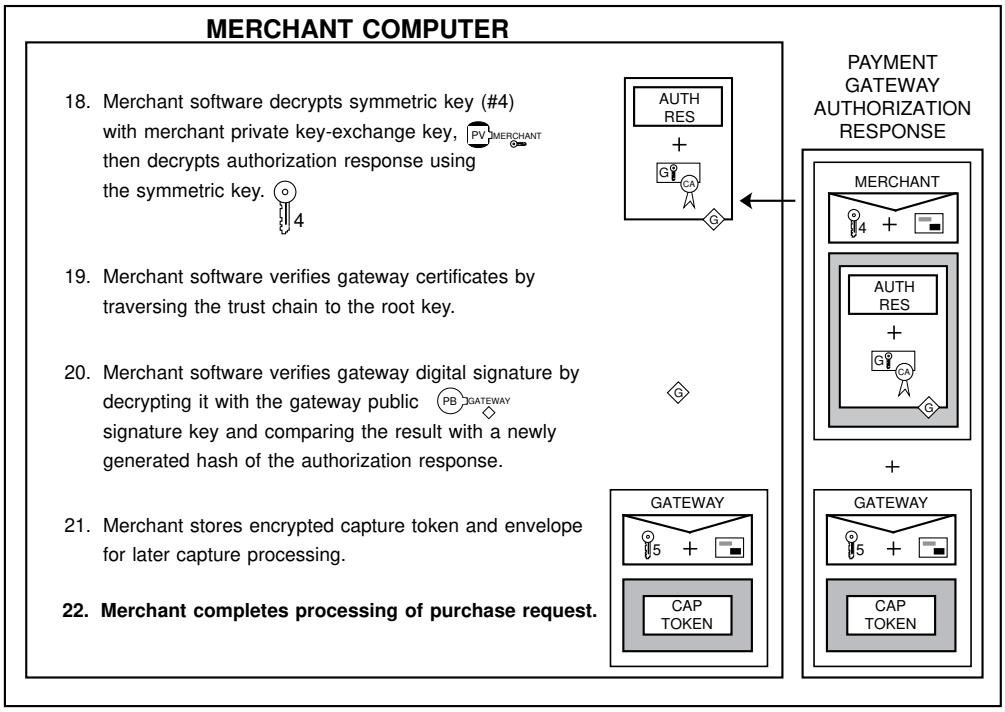
Continued on next page

4.5 Payment Authorization, continued

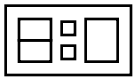
When the merchant software receives the authorization response message from the Payment Gateway, it decrypts the digital envelope to obtain the symmetric encryption key. It uses the symmetric key to decrypt the response message. It then verifies the Payment Gateway signature certificate by traversing 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 will store 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).

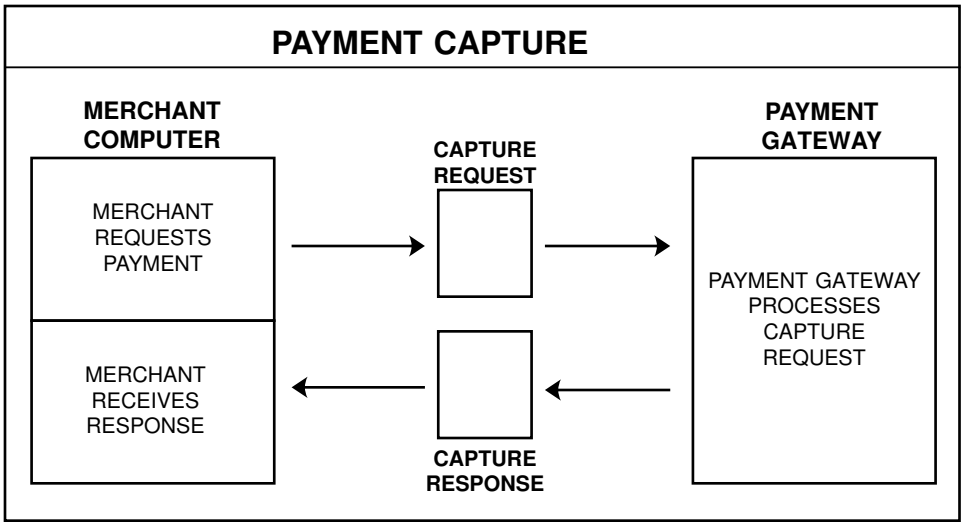
Merchant Processes Response



4.6 Payment Capture



The figure shown below provides a high level overview of a merchant's payment capture process. This scenario is divided into its three fundamental steps in the following detailed sections The icon to the left corresponds to the diagram below and serves as a map to this scenario; it is repeated in the explanations of the more detailed diagrams with a shaded region that indicates which step is being described.



Continued on next page

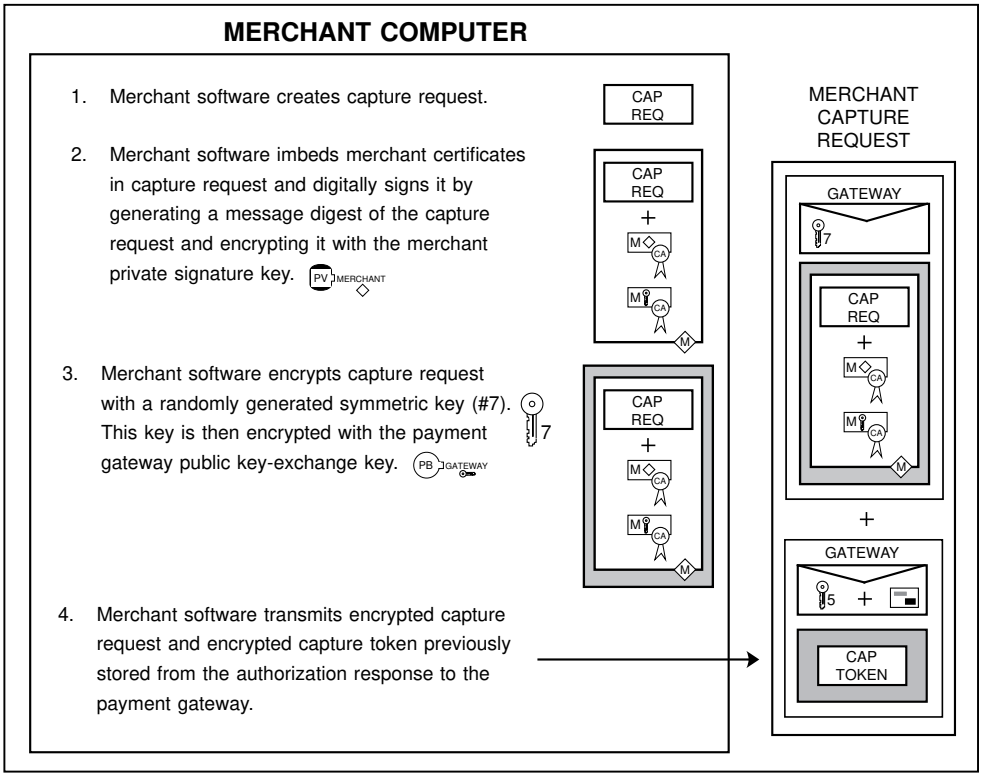
4.6 Payment Capture, continued

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.

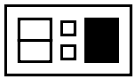
Note: while the flow described here contains only a single capture request, the merchant software is permitted to batch multiple requests into a single message.

Merchant Requests Payment



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.

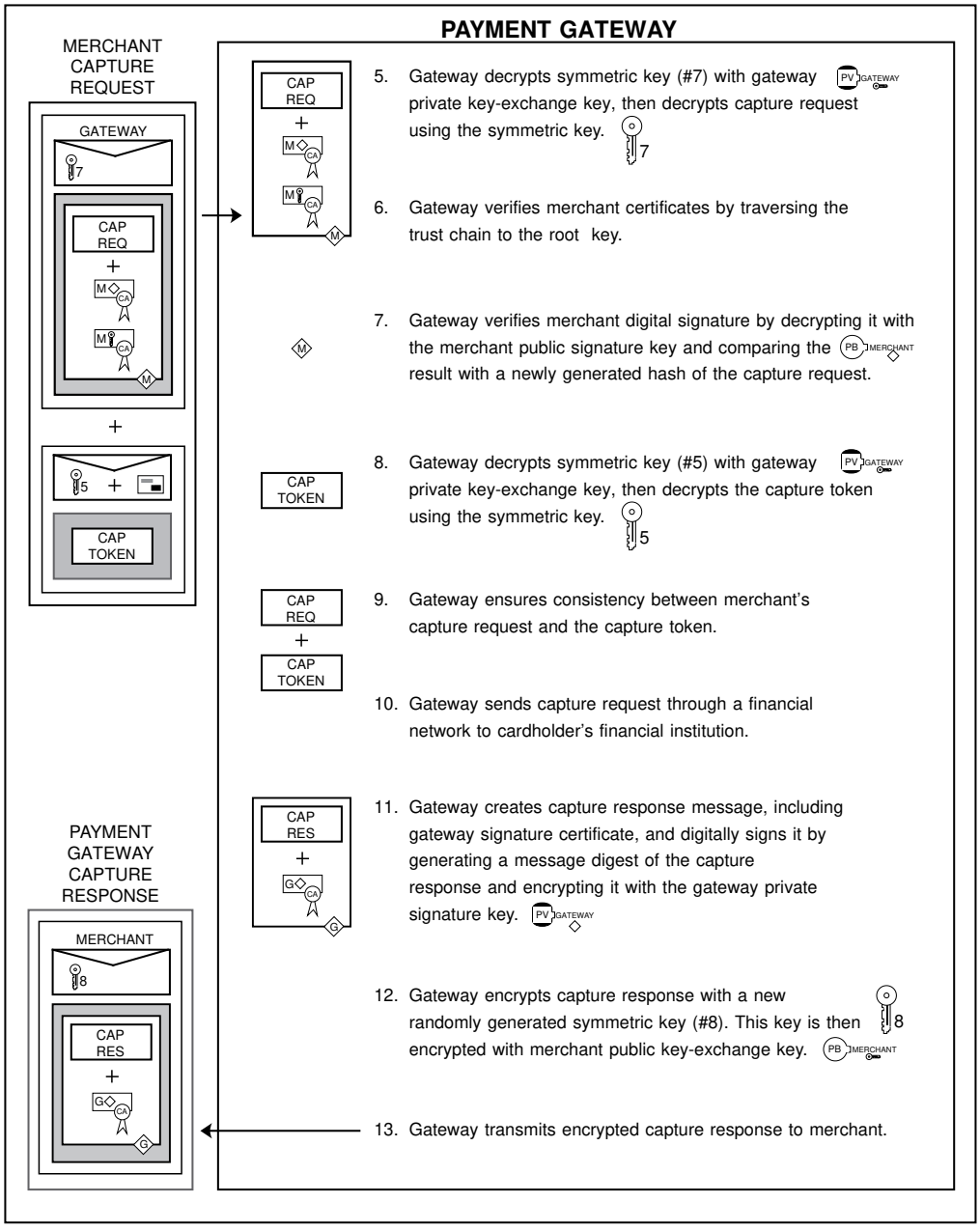
The Payment Gateway decrypts the capture token (if present) and then uses the information from the capture request and the capture token to format a clearing request, which it sends to the Issuer via a bankcard payment system.

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

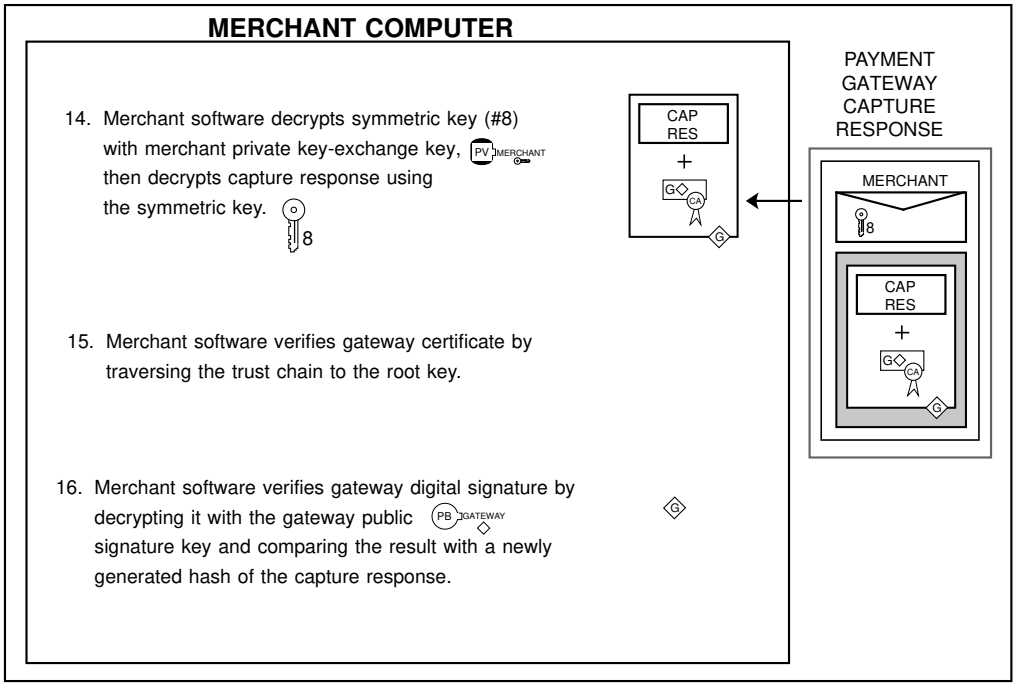
Payment Gateway Processes Capture Request



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 will store the capture response to be used for reconciliation with payment received from the Acquirer.

Merchant Receives Response