CHAPTER 1

Introduction to SET

This chapter gives an introduction to the SET Secure Electronic Transaction™ or SET™ protocol.

Chapter Roadmap

This chapter provides information on the following topics:

- An introduction to the basics and history of SET
- An introduction to shopping with SET
- Overview of the SET purchase transaction
- Some advanced SET-specific information

SET Basics

If you've made it this far, you are curious to know either what the SET protocol is, what it does, or how it does it. Each of these questions is answered in detail throughout the course of the book, but in their most basic terms, here are the answers:

What is SET? SET is a protocol designed to ensure that merchants and cardholders can conduct safe business over insecure networks — namely the Internet.

How does SET do it? SET uses cryptography to provide confidentiality and security, ensure payment integrity, and authenticate both the merchant and the cardholder. This security means that merchants are protected from purchases with an unauthorized payment card and can deny purchases to cardholders, banks are protected from unauthorized purchases, and cardholders are protected from merchant imposters or theft of their payment card numbers.

What does SET do? SET outlines a series of messages, as well as their contents and format, that are sent between the participants of an Internet transaction.

Electronic Commerce

As the World Wide Web's presence gets larger and more pronounced, we can expect to see some changes. Many of those changes have already started to happen. Traditionally, people had to either travel to a store or use Mail Order/Telephone Order (MOTO) to purchase goods and services, but every day people are starting to use the Internet to purchase these goods and services. A little of everything is available on the Internet—from books to travel arrangements; from music to computer software and hardware.

Electronic commerce uses an electronic form of cash, sometimes called digital or electronic cash, in order to purchase these goods and services. SET uses a payment system that is analogous to traditional payment cards—you purchase these goods and services and are billed from your payment card issuing bank. Numerous differences exist between traditional and electronic payment card shopping, but with electronic shopping the equivalent of your payment card is stored on your computer, and you can shop from the privacy of your own home. Every aspect of the transaction, from the cardholder's viewpoint, is handled from the cardholder's personal computer.

With electronic shopping, merchants are able to reduce overhead. The cardholders shop by themselves without the need of a salesperson or manager; the showroom is replaced with Web pages. Even if a store owner has no need to reduce overhead, the WWW's broad reach opens up a whole new collection of customers—and not only local customers, but global customers, too.

Precautions are taken by the SET software in order to ensure that transactions are handled in a safe manner that all but eliminates fraud and theft.

Announcement of SET

SET was officially announced on February 1, 1996. The announcement came from Visa and MasterCard (as well as others) and stated a convergence of their previously separate efforts. The original participants of the SET effort, along with Visa and MasterCard, were: GTE, IBM, Microsoft, Netscape Communications Corporation, SAIC, Terisa Systems, and Verisign.

The Participants

Before moving on to some more material about the SET protocol, I need to identify and explain the roles of some of the participants in a SET transaction. Each of the parties listed below plays an important role in a SET transaction.

Cardholder The cardholder is analogous to the average person who uses a payment card to purchase goods or services.

Merchant This is the business or organization who sells goods or services to the cardholder. In the case of a SET transaction, business with the merchant is performed electronically over the Internet.

Issuer The issuer is a financial institution that provides the cardholder with a payment card. The issuer's responsibility to guarantee payment on behalf of its cardholder. The issuer's processing is out-of-band from the perspective of SET, although it is still part of the transaction as a whole.

Acquirer The acquirer is the financial institution that processes payment card authorizations and payments for the merchant. The acquirer's responsibility is to obtain payment authorization from the cardholder's issuer.

Payment Gateway A payment gateway, or gateway, is an institution that works on the behalf of the acquirer to process the merchant's payment messages, including payment instructions from the cardholders. The gateway bridges communication between SET and the existing credit card networks.

Certificate Authority The certificate authority provides certification for the merchant, cardholder, and payment gateway. Certification provides a means of assuring that the parties involved in a transaction are who they claim to be.

Electronic Shopping vs. Traditional Shopping

At its most basic level, a SET transaction is similar to any other payment card transaction. Suppose that Aristotle is purchasing some items from Plato's Book Store (see Figure 1-1):

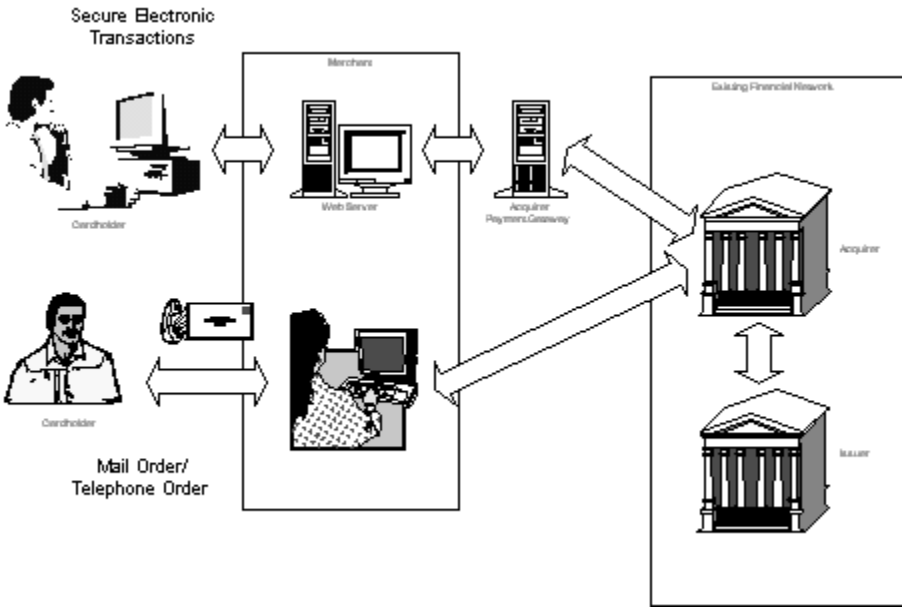

Figure 1-1 Electronic and traditional shopping. Copyright 1997 SET Secure Electronic Transaction LLC. Reprinted with permission. All rights reserved.

1. **The cardholder browses items the merchant has for sale.**

   Traditionally, Aristotle walks into a bookstore and browses items on the shelves. If he finds something that he likes, he puts it into his shopping cart.

   With electronic shopping, Aristotle uses his Internet browser to browse items Plato's Book Store has for sale on its Web pages. If he finds a book that interests him, he can add it to his virtual shopping cart. Plato's Book Store's Web site provides a mechanism for keeping track of the order state, thereby remembering which books Arisototle decides to keep in his cart.

2. **The cardholder decides which of the items to purchase.**

   With electronic shopping, as well as with traditional shopping, Aristotle can remove any or all of the books he has placed in his shopping cart. (This functionality is merchant-sup-

plied and is not a part of SET.) He pays only for the ones that he has decided to purchase.

3. **The cardholder is presented with an invoice containing the list of items and their price.**

   Traditionally, Aristotle takes his books to the cash register,and the clerk rings up his purchase and presents him with a total price.

   With electronic shopping, Aristotle makes his decision to pay via Plato's Book Store's Web site by clicking on a "Pay Now" button, or something similar. He is then presented with an sales order electronically, from the bookstore's server, or on his computer via his electronic shopping software.

4. **The cardholder selects a means of payment.**

   When standing at the checkout counter at the bookstore, Aristotle decides which of the credit cards in his wallet he wishes to use for his purchase.

   Similarly, Aristotle may have multiple cards he can choose from to complete his SET transaction.

5. **The cardholder gives the merchant order confirmation along with the means of payment.**

   Traditionally, this is as easy as Aristotle handing the clerk a credit card.

   With SET, the order and payment instructions are digitally signed by Aristotle and are then sent to the Plato's Book Store.

6. **The merchant requests authorization for the purchase.**

   With both electronic and traditional shopping, the bookstore sends an authorization request to its acquirer via it's payment gateway. The acquirer sends this information for processing to the Aristotle's issuer.

   The issuer returns with an authorization response. The response includes an indication of whether the authorization request has been approved. In turn, the acquirer responds to Plato's Book Store with the outcome (acceptance or rejection) of the processing.

7. **The merchant delivers goods to the cardholder.**

   The bookstore's clerk, in the case of traditional acceptance, gives Aristotle his books and sends him on his way. Arisototle will probably decide to have a fine cup of coffee and peruse his new books.

   In an electronic transaction, the bookstore makes arrangements to deliver the goods or services to Aristotle. These can be as simple as shipping his books to his home or office.

   This signifies the end of the transaction from Aristotle's viewpoint.

8. **The merchant's acquirer captures funds from the cardholder.**

   With both electronic transactions and traditional shopping, Plato's Book Store requests payment from the Aristotle's financial institution via its acquirer by submitting a capture request. The capture request is sent through the payment card network to the issuer.

Generally, the above steps define a purchase; however, there many variations on the business flow exist. Throughout the course of this book these variations will be identified and explained.

Shopping With SET

SET only formally addresses payment authorization and transport, order confirmation and inquiry, and merchant reimbursement. Arrangements are made by the merchant, the cardholder, and other third-party organizations by whatever means they choose to accomplish the other phases.

The following is a brief overview of what parts of the transaction that SET is directly involved in (the stages in bold are the parts of the transaction that are addressed by SET, the others are performed outside the SET protocol):

- Browsing and Shopping—The cardholder browses and shops a merchant's goods via merchant created and implemented Web pages, Web server, and back-end code. These pages, and the code used to perform such functions as keeping track of the cardholder's shopping state, are collectively referred to as the *shopping experience*.
- Merchant and Goods Selection—The cardholder (via the internet, a Web browser, and the World Wide Web itself) chooses which merchant s/he wishes to make a purchase from and browse that merchant's web site looking for products or services that interest him/her.
- Negotiation and Ordering—The cardholder chooses what goods or services s/he wishes to purchase, and agrees to pay the price that the merchant places on these goods and services.
- Payment Selection—The cardholder selects which payment card to use for the transaction. SET allows for the support for multiple credit card brands.

- **Payment Authorization and Transport**—The messages used for the authorization of payment from the cardholder to the merchant are sent between the proper participants.
- **Payment Confirmation and Inquiry**—The merchant or cardholder can inquire about the status of a purchase, or the purchase can be finalized via the financial institutions.
- Delivery of Goods—The merchant handles the shipment of goods, or the delivery of services, and makes arrangements to provide the cardholder with these goods or services.
- **Merchant Reimbursement**—The merchant is reimbursed by the cardholder. Payment reversal and credit may also happen at this time.

SET Purchase Transaction

Figure 1-2 shows what might happen in a SET purchase transaction in a little more detail. Things may not happen exactly this way, but in general, this is very typical of a SET purchase transaction from start to finish.

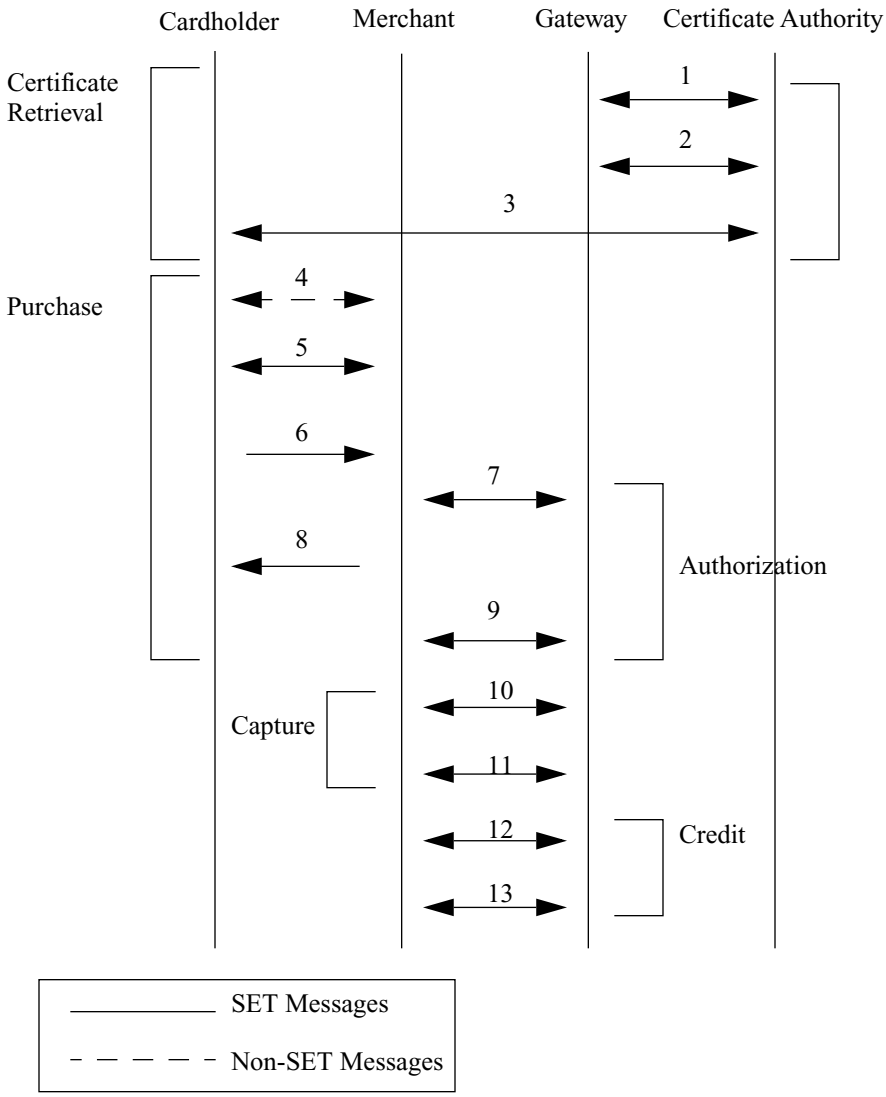

Figure 1-2 Basic transaction flow

Certificate Retrieval Before a transaction can start, each of the parties involved must obtain certificates. Certificates assist in the authentication process. The certification process is

explained in more detail in Chapter 4, *Certificates and Certification*.

1. The gateway obtains the certificates it needs from the certificate authority.
2. The merchant obtains its certificates from the certificate authority.
3. The cardholder obtains its certificates from the certificate authority.

Purchase These steps encompass what is normally thought of as the 'heart' of the transaction, even though other steps are involved in the purchase transaction as a whole. More information about this phase of the transaction can be found in Chapter 5, *SET Payment Messaging*.

4. The cardholder shops at the merchant's shopping experience and decides what goods or services s/he wishes to buy.
5. The merchant sends the cardholder certificates needed in the purchase transaction.
6. The cardholder sends a request to purchase the items that s/he has selected. This message contains information about the cardholder's order and the cardholder's payment information—such as the cardholder's card information. The merchant gets the order information and sends the cardholder's payment card information onto the payment gateway (see step #7). The merchant is never privy to the cardholder's payment information and therefore has no way of obtaining the cardholder's payment card information. This security measure is designed to protect the cardholder.
7. The merchant and payment gateway share authorization information. This consists of the merchant sending the payment gateway information such as the cardholder's payment card information and the amount of the transaction. The payment gateway can either authorize or decline the transaction based on the information received from the merchant. The amount authorized must be captured by the merchant later, and no money changes hands during the authorization phase.
8. The merchant sends a message to the cardholder 'finalizing' the transaction. The cardholder sees this as the end of the transaction.
9. This step is optional, but allows the merchant to change or eliminate money authorized in step #7.

Capture The capture phase handles capture of money that has been authorized in step #7. It also handles reversal of captured money, if needed. Money authorized is usually captured by the merchant in some predetermined regular time frame, such as at the end of every day. More information about this phase of the transaction can be found in Chapter 5, *SET Payment Messaging*.

10. The merchant and the payment gateway share capture information. A request is sent from the merchant to the gateway to capture money that has been authorized—this capture

request can be for a single authorization amount or multiple amounts. The gateway processes the capture request through its existing payment card financial network.

11. If an error has occurred capturing cardholder funds, messaging between the merchant and the gateway takes place in order to reverse the capture. This step is optional and only happens if there has been a capture error has occurred.

Credit Sometimes a merchant needs to credit a cardholder's account. These messages accomplish credit and credit reversal. More information about this phase of the transaction can be found in Chapter 5, *SET Payment Messaging*.

12. The merchant and payment gateway exchange messages in order to credit a cardholder's account.
13. If a credit has been granted by mistake, the merchant and payment gateway can exchange messages in order to reverse the granted credit.

Now that we have some of the basics out of the way, let's move on to some more advanced SET-specific material.

Interoperability

Interoperability ensures that each software vendor's solution for SET works with every other vendor's.

Interoperability is ensured through measures like the following:

- Message format is non-ambiguous, non-proprietary, and an open standard. All messages in SET are clearly defined by the SET Specifications.
- The method of message transport is not defined. How messages arrive is not important—what is important is that they *do* arrive.
- The content and encoding of messages is standard. (See the following sections in this chapter for more information about ASN.1 and DER.)
- SET employs the PKCS #7 standard for its cryptographic encapsulation. (See Appendix C, *PKCS #7 Formats*, or Chapter 3, *Encryption and Cryptography,* for more information about the PKCS #7 standard.)
- The SET Secure Electronic Transaction LCC organization handles testing SET standards compliance in order to grant SETMarks—which are a visible symbol that a piece of software complies with the SET Specification. (See Chapter 7, *SET Standards and Compliance*, for more information pertaining to SET standards and SET Secure Electronic Transaction LCC.)

Interoperability Testing

Currently, two different types of interoperability testing are available: payment flow testing and certificate flow testing. Payment flow testing determines whether cardholder, merchant, and gateway applications complete successful transactions using certificates from a common certificate authority. Certificate flow testing determines whether one vendor's applications can receive certificates from another vendor's certificate authority.

SET Messages

Messages are the heart of the SET protocol. Messages carry information between the entities in a SET transaction. As was mentioned previously, the messages in SET are non-ambiguous and non-proprietary—but what do those terms mean? Previously adopted standards are used to compose and encode the messages. SET has adopted the standard Abstract Syntax Notation 1 for its message content format, and Distinguished Encoding Rules for encoding the message into a binary format.

Message Wrapper

All SET messages are encapsulated within a SET message wrapper. The message wrapper is decoded by the receiving computer before any processing of the message is done. Message wrappers are described in more detail when applicable.

Abstract Syntax Notation One (ASN.1) — Message Content

SET uses ASN.1 to describe its abstract data types and values. ASN.1 is a non-ambiguous definition of the content of messages. With ASN.1 you can describe the format of complex objects by putting together more, simpler types. The product is broken down into its components.

In ASN.1, a *type* is considered to be a set of values. A *value* is an element of the type's set. For some types, a finite number of values exist, and for some types, an infinite number of values exist.

Types and values can be given names using the ASN.1 assignment operator (::=), and those names can be used in defining other types and values.

The following data types are used by ASN.1 in SET:

- BIT STRING—A field containing a sequence of zero or more bits
- BMPString—A field containing a sequence of Basic Multilingual Plan (BMP) characters
- BOOLEAN—A field containing a value of either TRUE or FALSE
- CHOICE—A field containing a union of one or more types
- CLASS—An intrinsic type used to define additional data types using simple type definitions and constraint rules
- ENUMERATED—A field whose value is bound to pre-defined identifiers

- GeneralizedTime—A field containing a string, a calendar date, and a time
- IA5String—A field containing a sequence of IA5 (ASCII subset) characters
- INTEGER—A field containing an integer number value
- NULL—A field containing a null value
- NumericString—A field containing a string of digits or space
- OBJECT IDENTIFIERS—A sequence of integers that identify an object
- PrintableString—A field containing a sequence of printable characters
- REAL—A field containing a real number value
- SEQUENCE—A type containing an ordered collection of one or more fields
- SET—A type containing an unordered collection of one or more fields
- TYPE-IDENTIFIER—An intrinsic type used to refer to the value of an OBJECT IDENTIFIER type by its unique identifier
- UniversalString—A field containing a sequence of universal characters
- UTCTime—A field containing a string, a calendar date, and a time using a two digit year
- VisibleString—A field containing a string of visible characters

ASN.1 uses a series of two hyphens (--) to signify a comment.

Distinguished Encoding Rules—Message Encoding

ASN.1 does not specify how these objects are encoded into strings of ones and zeros. For that, you must use a set of encoding rules. The two most common encoding rules are the Basic Encoding Rules (BER) and the Distinguished Encoding Rules (DER). The only difference between BER and DER is that multiple ways exist to encode objects in the BER, but the DER is a subset of the BER such that it offers only one possible way to encode each object.

ASN.1 Example

How about an example that will help explain ASN.1?

Essentially, a type is a sequence of components, and each of the components may or may not be another sequence of components. Assume that we have a type called a chapterType. The chapterType describes what is in a chapter of a book:

```
ChapterType ::= SEQUENCE {
    chapterText             IA5String,
    numberOfPages           INTEGER,
}
```

The ChapterType is a SEQUENCE, or a type containing an ordered collection of one or more fields. The fields can contain either a value or another set of values. These are easy to figure out—the ChapterType contains the chapter text and a number of pages.

The BookType makes use of this ChapterType:

```
BookType ::= SEQUENCE {
     title                  IA5String,
     numberOfChapters       INTEGER,
     chapterOne             [0] ChapterType,
     chapterTwo             [1] ChapterType OPTIONAL,
     chapterThree           [2] ChapterType OPTIONAL,
     numberOfPages          INTEGER
}
```

What about the chapter definitions? The chapters are called *tagged* types. Tags are indices that are put on various components, so that the message decoder knows what's what. Unlike names, these tags are made available to the decoder. There are two types of tags: explicit and implicit tags. An implicitly tagged type is a type derived form another type by changing the tag of the underlying type. Explicit tagging denotes a type derived from another type by adding an outer tag to the underlying type.

The ASN.1 notation for SET and the JPO extension are provided for you in the appendices at the end of the book. They are valuable tools for understanding SET.

Object Identifiers

Object Identifiers, or OIDs, are used in SET to uniquely identify a particular type of object. These OIDs can be found throughout the SET ASN.1. Several different classes of OIDs are defined by SET:

- Algorithm OIDs—identifiers used to identify the cryptographic operators that are applied to a SET messages
- Content OIDs—identifiers used to identify the PKCS message type used for the content of a SET messages
- Extension OIDs—identifiers used to identify the general class of the X.509 certificate extensions used in a SET message
- Attribute OIDs—identifiers used to identify the general class for the attribute types used in SET messages
- ASN.1 OIDs—identifiers used to identify each of the ASN.1 modules for SET
- External OIDs—identifiers used to uniquely identify the higher-level OIDs referenced by SET and previously established by other organizations

SET Error Processing

SET defines a series of error messages that are used when an error occurs processing any of the normal messages of SET. The recipient of a SET message generates an error when the message fails format or content verification. When the message fails, an error is sent from the recipient of the message to the sender.

The error message is not intended to indicate a failure of a process (like a declined authorization), but it is rather there to indicate a failure in content or verification—the message, rather than the result, has a problem.

Four different categories of SET error messages exist:

- Duplicate message—Enough information appears in the mesage wrapper that a receiving entity can detect if a message is a retransmission or not. If the message being retransmitted is not designed to be transmitted more than once, the recipient can generate an error.
- Corrupted messages—A corrupted message cannot be parsed correctly by the receiving entity.
- Malformed messages—These happen when the message can be parsed, but is otherwise illegal due to the fact that the values are out of the expected range.
- Failed cryptography—If a message is received in which authentication tests fail, an error message is returned to the sender.