Master Card/Visa Secure Electronic Transaction

In August 1996, Master Card and Visa agreed to jointly develop the Secure Electronic Transaction (SET) Specification. This chapter includes a portion of this specification for pedagogical reasons. The specification has three parts:

- Book one: Business specifications
- Book two: Technical specifications
- Book three: Formal protocol

This chapter covers the following topics:

- Introduction
- Business requirements
- Concepts
- Payment

Introduction

Impact of electronic commerce

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

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

Projected use:

With more than 30 million users in 1998, and 90 million users projected to come onboard in the next two years, the Internet is a new way for business 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 Internet. 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, payment 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.

**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.

**Role of payment systems**

Payment system and their financial institution will play a significant role by establishing open specification for payment card transaction that:

- Provide for confidential transmission,
- Authenticate the parties involved,
- Ensure the integrity of payment instruction 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 community’s networks, procedures must be developed to substitute for existing procedures used in face-to-face or mail order/telephone order (MOTO) transaction including the authentication of the cardholder by the merchant.

**Use of payment card 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 payment card products instead of cash or checks. This will hold true both in the consumer marketplace and in the commercial marketplace.

**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 specification will enable greater payment card acceptance, with a level of security that will encourage consumers and business to make wider use of payment card products in this emerging markets.
Objectives

Motivation

The primary motivation for the bankcard association to provide specification for secure payments are:

- To have the bankcard community take a leadership position in establishing secure payment specification and, in the process, avoid any cost associated with future reconciliation of implemented approaches,
- To respect and preserve the relationship between merchants and Acquires 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 bankcards brands.

Payment security:

The objectives of payment security are to:

- Provide authentication of cardholders, merchants and acquires,
- Provide confidentiality of payment data,
- Preserve the integrity of payment data, and
- Define the algorithms and protocol necessary for these security services.

Interoperability:

The objectives interoperability are to:

- Clearly define detailed information to ensure that applications developed by one vendor will interoperate with application developed by other vendors,
- Create and support an open payment card 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 combination of hardware and software platforms such as power pc, Intel, Spare, UNIX, MS-DOS,OS/2, windows and Macintosh.

Market acceptance:

The objectives of market acceptance are to:

- Achieve global acceptance, via ease of implementation and minimal impact on merchant and cardholder and users,
- Allow for “bolt-on” implementation of the payment protocol to existing client application,
- Minimize change to the relationship between acquires and merchants, and cardholders and issuers,
- Allow for minimum impact to existing merchants acquire and payment system application and infrastructure, and
• Provide and efficient protocol view from the financial institution perspective.

Business requirement

Requirements

Introduction

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

Security issues noncompetitive:

Security issues regarding electronic commerce must be viewed as noncompetitive in the interest of financial institution, 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 payment card account.

4. Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution.

5. Ensure the use of the best security practices and system design techniques to protect all legitimate parties 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.

Features

Features of the specification:

These requirements are addressed by the following of these specification:

• Confidentiality of information
• Integrity of data
• Cardholder account authentication
• Merchant authentication
• Interoperability
Confidentiality of information:

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

Online shopping: In today’s online shopping environment, payment instructions containing account information are often transmitted from cardholders to merchants over open networks with little or no security precautions.

Fraud: While it is possible to obtain account information in other environments, there is a heightened concern about the case 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 out of a data stream), and the potential for “mischievous” fraud that appears to be characteristic of some hackers.

Confidentiality is ensured by the use of message encryption.

Integrity of data:

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

Payment information, sent from cardholders to merchants include order information, personal data and payment instructions. If any component is altered in transit, the transaction will not be processed accurately.

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 payment card account number. A mechanism that uses technology to link a cardholder to specific payment card account number will reduce the incidence of fraud and therefore the overall cost of payment processing.

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

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

Merchant authentication:

The specification must provide a way for cardholders to confirm that a merchant has a relationship with a financial institution allowing it to accept payment cards. Cardholders also need to be able to identify merchants with whom they can securely conduct electronic commerce.
Merchants authentication is ensured by the use of digital signatures and merchants certificates.

**Interoperability:**

The specification 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 merchants software that also meets the defined standard.

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

**Scope**

**Use of payment cards**

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

**Electronic shopping experience**

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

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

**With in 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 message and object formats
- Authorization message and object formats
- Capture message and object formats
- Message protocols between participants

**Outside the scope**

The following are outside the scope of the set specifications

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

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 acquire. However, in the electronic processing of the transaction begins with the cardholder.

Cardholder

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

Issuer

An issuer is the financial institution that establishes an account for a cardholder and issues the payment card. The issuer guarantees payment for authorized transaction using the payment card in accordance with payment card brand regulation 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 payment cards must have a relationship with an Acquirer.

Acquirer

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

Payment gateway

A payment gateway is a device operated by an Acquirer or a designated third party that processes merchant payment messages(including payment instruction form cardholders)

Brand

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

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

Third parties

Issuers and Acquires sometimes choose to assign the processing of payment card transaction to third party processor, this documents does not distinguish between the financial institution and the processor of the transaction.
Cryptography

Protection of sensitive

Cryptography has been used for centuries to protect sensitive information as it transmitted from one location to another in a cryptographic system in a message encrypted using a key.

Secret key cryptography

Secret key cryptography also known as symmetric cryptography, uses the same key to encrypt and decrypt the message.

Public key cryptography

Public key cryptography, also known as asymmetric key 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 the data encrypted with either key can only be decrypted using the other.

Encryption

Relation of keys

When two key users want to exchange messages securely, each transmits one component of their key pair, designated the public key, to the other and keeps secret key the other component, designated the private key.

Use of symmetric key

SET will rely on cryptography to ensure message confidentiality to SET, message data will initially be encrypted using randomly generated symmetric encryption key.

Digital signature

Relationship of keys

Because of the mathematically 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 private key. Any recipient can determine that the message came from the sender by decrypting the message using the sender’s public key.

Using message digests

When combined with message digests, encryption using the private key allows users to digitally sign message. A message digest is a value generated for a message for document that is unique to that message.

Two key pairs

SET uses a distinct public/private key pair to create the digital signatures. Thus, each SET participants 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.
Certificates
Authentication is further strengthened by the use of certificates

Need for authentication
Before two parties use public key cryptography to conduct business each wants to be sure that the other party is authenticated. Before Bob accepts a message with Alice`s digital signature, he wants to be sure that the public key belongs to Alice and not to someone masquerading as Alice on an open network

Need for trusted third party
An alternative to secure transmission of the key is to use a trusted third party to authentication that the public key belongs to Alice.

SET authentication:
The means that a financial institution uses to authenticate a cardholder or merchant is not defined by these specifications. each payment card brand and financial institution will select an appropriate method.

Certificate issuance
Cardholder certificates
Cardholder certification function as an electronic representation of the payment card because they are digitally signed by a financial institution, they cannot be altered by a third party and only the financial institution can generate one

Merchant certificates
Merchant certificates function as an electronic substitute for the payment brand decal that appears in the store window.

These certificates are approved by the acquiring financial institution and provide assurance that the merchant holds a valid agreement with an Acquire.

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

Acquirer certificates
An acquirer must have certification in order to operate a certificate authority that can accept and process certificate requests directly from merchants over public and private networks.

Issuer certificates
An Issuer must have certificates in order to operate a certificate authority that can accept and process certificate requests directly form cardholders over public and private networks.
Hierarchy of trust

SET certificates are verified through a hierarchy of trust. Each certificate is linked to the signature certificates of the entity that digitally signed it.

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.

Root key replacement

When the root key is generated, replacement key will 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.

Kinds of shopping

Variety of experiences

There are many ways that cardholders will shop. This section describes two ways.

Online catalogues

The growth of electronic commerce can largely be attributed to the popularity of the world wide web.

Electronic catalogues

Merchants may distribute catalogue on electronic media such as diskettes or CD-ROM.

Payment processing

Transaction described

This section describes the flow of transaction as they are processed by various systems:

- Cardholders registration
- Merchant registration
- Payment authorization
- Payment request
- Payment capture
Other transaction

The following additional transaction are part of these specification but are not described in this section.

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

Protocol description

In this event that the description of the processing in this section differs from the formal protocol definition. The formal protocol definition take precedence.

Certificate authority function

- Receive registration requests
- Process and approve/decline requests and
- Issue certificate

The following list presents some suggestion 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 process and approves certificate request for its cardholders or merchant and forwards the information to the appropriate payment card brand to issues the certificates.
- Certificate requests are received by an independent Registration Authority that process payment card certificates application for multiple payment card brands and forwards requests to the appropriate financial institution (issuer or acquirer) for processing; the financial institution forwards approved requests to the payment card brands to issues the certificates.

Optional cardholder certificates

The diagrams and processing flows that describes the processing of the transaction when the cardholder is in possession of a signature.

No digital signature

When a cardholder does not possess a signature certificate no digital signature is generated. In place of the digital signature, the certificate generates the message digest of the data and inserts the message 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 payment card brand and the payment card issuer to authenticate the cardholder prior to the certificate being issued.

Cardholder authentication

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

Cardholder registration

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

Cardholders must register with a Certificate Authority before they can send SET message 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.

- Cardholder initiates registration
- Certificate authority sends response
- Cardholder receives response and request registration forms
- Certificate authority processes request and sends registration form
- Cardholder receives registration form and request certificate
- Certificate authority processes request and creates certificate
- Cardholder receives certificate

Merchant registration

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

Merchant must register with a certificate authority before they can receive SET payment instruction from cardholders or process SET transaction through a payment gateway. In order to send SET message 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.

- Merchant request registration form
• Certificate authority process request and send registration form
• Merchant receives registration form and request certificates
• Certificate authority process request and creates certificates
• Merchant receives certificates

Purchase request

The figure shown below provides a high level overview of the purchase request portion of a cardholder 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 explanation of the more detailed diagrams with a shaded region that indicates which step is being described.

• Cardholder initiate request
• Merchant sends certificate(s)
• Cardholder receives response and sends request
• Merchant process request message
• Cardholder receives purchase response

Payment authorizations

The figure shown below provides a high level overview of a merchant 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 explanation of the more detailed diagrams with a shaded region that indicates which step is being described.

• Merchant request authorization
• Payment gateway process authorization request
• Merchant process response

Payment capture

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

• Merchant request payment
• Payment gateway process capture request
• Merchant receives response
E-MAIL AND SECURE E—MAIL TECHNOLOGIES FOR ELECTRONIC COMMERCE

Introduction:-

E-mail is the use of electronic messaging technologies to allow computer users to communicate with each other for a variety of purposes. An electronic message can consist of a single text line: of a multimedia document encompassing text, video, and sound; or some other document. E-mail supports messaging, return receipts, and the ability to attach pertinent ancillary files to the basic message.

E-mail allows one to transmit messages and other files to people located either down the hallway, or, using the Internet, around the world. In order to send Internet mail, one needs to obtain an account with an Internet Service Provider or an on-line service (i.e., America Online, Prodigy, and so forth) and know the address of the recipient. The ISP provides an Internet address to the subscriber that allows the individual to receive Internet mail.

Companies are using the Internet to pursue business opportunities in three areas; electronic collaboration, information distribution and access, and electronic commerce.

- Message can be sent to multiple parties simultaneously and nearly instantaneously without having to retype each individual letter or memo.
- Someone receiving a message may forward the message to another destination with or without comment. Mail can be sorted in order to determine what to read immediately and what to read later.
- Message can be filed electronically for future reference.
- There are simplified procedure for responding to mail sent by others.
- Mail can be accessed and sent from anywhere around the world. This feature becomes even more prevalent in today’s working society because of telecommuting. Many companies find telecommuting attractive because they save on benefits and overhead or office space as part of the virtual corporation discussed in Chap.1
- Multiple copies can be sent in different formats. Messages can be sent electronically to another mailbox, a telex terminal, another fax machine, by mailgram or cablegram, or all at once. Attachments of all kinds can (generally) be included.
**The Means of Distribution:**

Electronic mail and messaging systems are an increasingly important part of an enterprise’s computing and communications strategy. E-mail can be distributed over a private enterprise network, on-line networks (such as AOL), and the Internet. The growth in the subscriber population of Internet – based services for both individuals and businesses, makes Internet e-mail pervasive tool.

Most companies using the Internet for electronic commerce of EDI use mail communication with customers and business partners, they also use FTP for accessing public archives and for delivering software patches. As described elsewhere, the Internet provides a variety of capabilities for e-commerce/EDI use, including e-mail, file transfer, World Wide Web, and remoter logins. TCP/IP provides the underlying transport protocol; the applications support different protocols, dependent on function. For example, a business application may need to utilize SMTP for mail, FTP for file transfer, HTIP for World Wide Web access, and Telnet for remoter logins. Each of these protocols supports different capabilities with respect to use and value-added functions such as security, encryption, and non repudiation.

The Internet Engineering Task Force (IETF) meets regularly to discuss operational and technical issues impacting the Internet community. Capabilities related to security are under development or have recently been development by the IETF. Working groups are set up for further investigation of important issues. Anyone can attend either of theses meetings and become a member of a working group. Each working group has the responsibility of producing documentation and deciding how issues should be handled. The reports are called RFCs (Requests for Comments). To obtain an RFC, one can send a mil message to rfc-info@isis.edu with a message body of

```
Retrieve : RFC
Doc- ID : RFCxxxx
```

where xxxx is the number of the RFC.

**A Model for Messages Handling:**

In 1971, the International Federation for Information Processing, a pre standards organization, developed a model for messages handling. This model was eventually adopted and expanded by the International Telecommunication Union- Telecommunication (ITC-T), which developed the X.400 series recommendations, Message Handling System (MHS). Although Internet mail is not based on ITU-T standards, it is useful to look at this abstraction.
• The envelope is meaningful to the message transfer agents.
• The headers are meaningful to the user agents.
• The body is meaningful to the users (people or programs).

Upon successful completion of the submission protocol, the MTA accepts the responsibility to deliver the e-mail messages or, if delivery fails, to inform the originating user of the failure by generating an error report.

If not, it contacts an adjacent MTA that is closer to the recipient and negotiates transfer of the e-mail message. This process repeats until some MTS determines that the message is undeliverable. Given this model for e-mail, one realizes that:

• E-mail transfer is *third-party* in nature. Once an e-mail message passes through the posting slot, the user agent has no claims on the message. The MTS takes responsibility for the e-mail message of posting time and retains that responsibility until delivery time.
• E-mail transfer is *store-and-forward* in nature: the UAs for the originator and recipient need not be on-line simultaneously for mail to be submitted, transported, and delivered. In fact, only the node currently responsible for the e-mail message and the “next hop” taking responsibility for the message need be connected in order for the message to be transferred.

The summarize, there are three general protocols involved in the model:

- A messaging protocol used between two UAs.
- A relaying protocol used between two MTAs.
- A submission/delivery protocol used between an MTA and UA.

**Internet Apparatus:**

We can view the Internet suite of protocols used for generic transmission as having four layers:

1. The *interface* layer describes physical and date-link technologies used to realize the transmission at the media (hard ware) level.

2. The *internet* layer describes the internetworking technologies used to realize the internetworking functions; this is realized with a *connectionless-mode* network
service, provided by the Internet Protocol (IP), originally defined in 1981 in RFC-791.

3. The transport layer describes the end-to-end technologies used to realize communications between systems; this is realized with a connection-oriented transport service provided by the Transmission Control Protocol (TCP), originally defined in 1981 in RFC-793.

4. The application layer describes the technologies used to provide end-user services. The Internet protocols related to mail-specific applications are as follows:

- The Simple Mail Transfer Protocol (SMTP), defined in RFC-821 (August 1982) and RFC-974 (January 1986), which provides store-and-forward service for textual e-mail messages, and RFC-822 (August 1982), which defines the format of those messages.

- The Post Office Protocol (POP), Defined in RFC-1225 (May 1991), which provides a simple mailbox retrieval service.

- The Network Transfer Protocol (NNTP), Defined in RFC-977 (February 1986), which provides store-and-forward service for news messages.

- The Domain Name System (DNS), Defined in RFC-1033 (November 1987), and RFC-1034 (November 1987), which provides mapping between host names and network addresses.

**How does e-mail works:**

The first architecture is commonly referred as a file-based system. In this architecture, the mail clients creates a file containing the message header, text, and pointers to attachments and posts it to a directory on a post office server. Next, message transport software, usually hosted on another PC, uses TCP/IP transport capabilities to route messages from post office to post office, as needed. The recipient’s e-mail client periodically polls the local post office server’s directory and notifies the user when new mail arrives.

The second example is more popular client/server architecture here. The first step involves the e-mail client workstation creating a real-time session with an e-mail server and using a remote procedure call (RPC) to request an `ID that will be used to label the message envelope.

**Delivery date:**

This line shows the date and time the message was received in the mailbox.

**Return Path:**

This line shows the reply address of the original sender.
Received:

Every entry in the header starting with received represents a computer/gateway that has transferred the message also referred to as a hop. If there are too many hops, the message will be bounced or returned to the original sender. A message will also bounce if the person is no longer found at that mail system.

Date:

This line shows the date and time the message left the sender. This will vary by several seconds or minutes from the delivery date line.

From: This line specifies the full name and email address of the original sender.

Message ID:

This line serves as a unique identifier of each mail message. It includes the name of the machine sending the message, the date, time and file name.

To:

Each person receiving the message will appear on the line if there is more than one address, the addresses will be separated by a comma.

For example, an internet address is denise_derkacs@merck.com. The user name is denise_derkacs. The domain is merck.com.

.edu for educational institutions
.gov for federal governmental officers are organization
.org for any other address that does not fall into a previous identifiers, usually non profit organization

Address outside the United States will append a two-letter country identifier, such as .ca
MIME: MULTIPURPOSE INTERNET MAIL EXTENSIONS

BASIC CONCEPT

Multipurpose internet mail extensions (MIME) RFC-1521 provides internet e-mail support for messages containing formatted text, sound images, video, and attachments

- Common way in which files are sent as e-mail on the internet.
- Content type are
  1. Primary type----indicates general content of the material
  2. Subtype ___indicates the specific format.
- Five basic primary mime content types of text, image, audio, video, and application
- Composite MIME content types
- Message: one can send the message inside another message, labeling it message/rfc822. A mime mailer can label each segment or part of the message as message/partial. The recipients mail software can reassemble the message automatically.
- Multipart: allows more than one piece of MIME to be included in a message.
- MIME encoding
  - Uses many different encoding methods, depending on the file type it is sending.
  - Content _transfer_encoding header on each message corresponding to the type of decoding the recipient needs to perform.
  - Mime software adopts the general philosophy of trying to work with existing non-MIME software as much as it possibly can.
  - Users an encoding called base 64 for pure binary files.

Figure depicts the RFC-822 mime transport envelope. The multipart/signed content type contains two body parts. The first body parts is the body part over which the digital signature was created, including its mime headers. The second body parts contains the control information necessary to verify the digital signature.

When creating a multipart signed body part, the following sequence of steps describes the processing necessary.

1. The content of the body part to the protected is prepared according to a local convention. The content is then transformed into a mime body parts is canonical mime format, including an appropriate set of mime headers.
2. The body part to the digitally signed is prepared for signature according to the value of the protocol parameter.
3. The prepared body part is made available to the signature creation process according to a local convention. The signature creation process must make available to a mime implementation data streams.

When receiving a multipart/signed body part, the following sequence of steps describes the processing necessary to verify the signature are signatures.

1. The first body part and the control information in the second body part must be prepared for the signature verification according to the value of protocol parameter.
2. The prepared body part must be made available to be signature verification process according to a local convention.
3. The result of the signature verification process is made available to the user and the
mime implementation continuous processing with the verified body part.

**When creating a encrypted body part**

1. The content of the body part to be protected are prepared to a according to a local
   convention. The content are then transformed into a mime body part is canonical
   format.
2. The body part to be encrypted is prepared for encryption according to the value of
   the protocol parameter.
3. This prepared body parts made available to the encryption process according to their
   local convention. The encryption process must make available to a mime
   implementation two data streams.

**When receiving a multipart/encrypted body part**

1. The second body part and the control information in the first body part must be
   prepared for the decryption process according to the value of the protocol parameter.
2. The prepared body part must be made available to the decryption process according
   a local convention.
3. The result of the decryption process is made available to the user and the mime
   implementation continuous processing with the decrypted body part.

**MIME body part**

Mime specification currently support seven body types

Text, multipart, application, message, image, audio and video.

**TEXT:** The text body part enables a message to contains simple message data such as
ASCII and can be transported using the current seven bit ASCII used on internet. This the
most rudimentary form of message content specified within MIME.

**Multipart:**
the multipart body consist of several body parts containing unrelated data. Mime permits
the user to break the content of down into subtypes the four initial subtypes are mixed,
alternative, parallel and digest.

**mixed**
the mixed multiple body parts subtypes is the most frequently used it is ensures that a
number of very different message content types such as text, graphics, or images can
transmitted in the same message.

**Alternative:**
this subtype presents the same date in different such as word processing documents
in three representations such as ascii word for windows and word perfect.

**parallel**
this subtypes contains body parts that must be viewed at same time. This type is
used to when documents are linked with a utility such as hypertext.
digest

this subtype is used when all the body parts are messages in their own right.

MESSAGE:

A message body parts contains other messages such as forwarded or transfer messages. Is the most basic body part MIME, and its subtype are as follows

- RFC822
- PARTIAL
- EXTERNAL BODY

IMAGE:

The images body part contains time varying images and image that contain movement like motion pictures and full motion video

MPEG:

Motion pictures expert group(mpeg) is the standard digitally compressing movies.

GIF:

CompuServe’s graphics image format.

AUDIO:

The audio body part contains sound data such as views voice or music. The basic subtype indicates 8-bit, integrated service digital network(ISDN).

APPLICATION:

Application body parts contains generated from computer application program, contains spreadsheets, calendar information, word processing documents, and presentation format such as word perfect or Microsoft word.

OCTET-STREAM:

This subtype used for binary data that does not need or have an interpreter.

ODA:

This subtype is the office document architecture as defined by international communication union.

POST SCRIPT:

This subtype is defined by adobe system and support high quality post script printer output this uses with nonprinter interpreters because the information obtained in a postscript file that sending this format may the receiver information about the senders access to files.

MIME DATA ENCODING TECHNIQUES:

The current SMTP network only supports the seven bit ASCII, upto thousand characters per line of data, and a normal message length of 64kb. Longer messages are possible after being
segmented into manageable parts, but the maximum length that will go through any gate way is still 64kb.

**BASE 64**

Base 64 for is for any series of octets and its used in private enhanced messaging (PEM), Specified in RFC1113. This encoding takes a series of 3-octets and output 4-ASCII characters to represent them.

**8-BITS:**

8-bits means that lines are of the same form as they are in seven bit encoding.

**BINARY:**

Binary means that there is not a line length limit within the message. it also means that the body has not the encoded.

**Quoted printable encoding**

This encoding value is for data that generally uses on ASCII character set. Instruction on how to establish this type of contained in RFC -1521.

**7-bit**

7-bit is the default value when the content transferred encoding header field is not present in the header.

**x-token**

this value is for defining a non standard encoding which has been put in place by mutual agreement between the parties is the transfer.

**S/MIME: SECURE MULTIPURPOSE INTERNET MAIL EXTENTION**

Without any built in privacy, an internet e-mail message is very much like a postcard. Everyone who touches the postcard has the opportunities to read the entire content of the message.

In July of 1995, a group of leading networking and message vendors, in conjunction with cryptography developer RSA Data Security endorsed a specification that enables encrypted message to be exchanged between e-mail application from different vendors.

While sophisticated encrypted and authentication technology has been viewed as a crucial enabling technology for electronic commerce over the world wide web, only a few email packages offer security. Although Internet Privacy Enhanced Mail is excellent for text-based messages, MIME represent the next generation and has been widely adopted because of its ability to handle nearly any content type.

Proponents expect "S/MIME” to be the de-facto standard vendor independent e-mail encryption.

S/MIME was designed to add security to e-mail message in MIME format.

**What is S/MIME :** S/MIME is a specification for secure electronic mail. S/MIME was designed to add security to e-mail messages in mime format.
Why S/MIME there is a growing demand for e-mail security. S/MIME melds proven cryptographic constructs with standard e-mail practices.

Is S/MIME a standard? At press time the S/MIME working group plans to submit the S/MIME specification to the IETF for consideration as an official Internet RFC standard as soon as interoperability tests are complete.

How does S/MIME compare with PGP and PEM? S/MIME, PGP and PEM all specify methods for securing electronic mail.

PGP can be thought of as both a specification and an application. PGP relies on users to exchange keys and establish trust in each other.

How does it compare with MOSS?

Comparing S/MIME with MOSS, one should note that the letter was designed to overcome the limitation of PEM. By handling mime message or being more liberal in the hierarchical requirements.

What cryptographic algorithm does S/MIME use?

S/MIME uses a hybrid approach to providing security, often referred to as a digital envelop. The bulk message encryption is done with a symmetric cipher, and a public key algorithm is used for key exchange.

What are the PKCS, particularly PKCS 7 and PKCS 10?

PKCS (public key cryptography standard) is a set of standards for implementation of public-key cryptography. It has been issued by RSA Data Security in cooperation with a computer industry consortium.

Does S/MIME use digital certificates?

S/MIME use does use digital certificate the x0509 format is used due to its wide acceptance as the standard for digital certificates.

Does S/MIME only work on the internet?

S/MIME is not specific to the internet and can be used in any electronic mail environment. Consideration was given so that the smaller, private implementation could grow to become part of the internet. This is accomplished by making the implementation guidelines flexible and scalable.

Is a public domain implementation of S/MIME available?

A free version of S/MIME was planned to be available soon.

Are there any tools available for building S/MIME clients?

RSA tool kit for interoperability privacy enhanced messaging is S/MIME compatible. TIPERM is a tool kit is designed for developers.
MOSS :Message Object Security

Purpose

MIME object security service defined in RFC-1848 is a protocol used to apply digital signature and encryption services to MIME object. The services are offered through the use of end to end cryptography between an originator and a recipient, at the application layer.

Private key is used to digitally signed MIME object. The recipient of the message uses the stored originators public key to verify the digital signature.

MOSS Service overview

The moss digital signature service

The moss digital signature service requires two components:

The data is to be digitally signed and time private key of the originator. The digital signature is created by generating a hash of the data and encrypting the hash value with the private key of the message originator.

1. The body part to be signed must be converted to a canonical form that is uniquely and unambiguously represented in both environment in which it was created and the environment which it will be verified.
2. The digital signature and other control information must be generated. Some control information that is generated by the digital signature services is a version of the moss protocol.
3. The control information must be in cooperated in an appropriate mime content type. The application / moss signature content is used on the second body part of an encoding multipart/signed it must include the digital signature of the data.
4. The control information body part and the data body part must be incorporated in a multipart/signed content type.

The MOSS encryption service:

The MOSS encryption service requires three components:

The data to be encrypted

Data encrypting key to encrypt the data

The public key of the recipient

1. The body part to be encrypted must be in MIME compliant form.
2. The data-encrypting key and other control information must be generated. The application of the encryption service generates control information which includes the data encrypting key used to encrypt data itself.
3. The control information must be incorporated into an appropriate MIME content type. See step 3 under MOS digital signature service the application-keys content type is used on the first body part of an enclosing multipart/encrypted.
4. The control information body part and the encrypted data body part must be incorporated into a multipart/encrypted content type. See step 4 under MOSS digital
signature service. The definition of the multipart/encrypted body part in RFC-1847 specifies three steps for creating the body part.

**The multipart/encrypted content type is constructed as follows.**

- The value of its required parameter protocol is set to applications/moss-keys.
- The first body part is labeled applications/moss-keys and is filled with the control information generated by the encryption service.
- The encrypted body part becomes the content of its second body part, which is labeled application/octet-streams.

**Definition of security subtypes**

- Multipart/signed
- Creating process of multipart/signed
- Receiving and verifying process of multipart/signed
- Multipart encrypted
- Creating process of multipart/encrypted
- Receiving and verifying process of multipart/encrypted

**Application MIME object security service**

**Digital signature service**

The verification of the MOSS digital signature service requires the following components:

- A recipient to verify the digital signature.
- A multipart/signed body part with two body part: the signed data and the control information.
- The public key of the originator

The definition of the multipart/signed body part is RFC-1847 species three steps for receiving it.

**Encrypted service:**

- A recipient to decrypt the data
- A multipart/encrypted body part with two body parts the encrypted data and the control information
- The private key of the recipient

The definition of the multipart/encrypted body part in RFC-1847 specifies three steps for receiving it:

- The encrypted body part and the control information body part are prepared for processing
- The prepared body parts are made available to the decryption process
- The results of the decryption process are made available to the user and processing continues with the decrypted body part, as returned by the decryption process.

**Key management content types**
The key management function are based on the exchange of the body parts two content types are used:

Application/mosskey-request content type:

The user would use this content this to specify needed cryptographic key information. The message containing this content type might be directed toward an automatic or manual responder.

Application/mosskey-data content type:

The principal objectives of this content type is to convey cryptographic keying material from a source to a destination.

Pretty good privacy (PGP)

Pretty good privacy, already introduce in chap.s, is a public key encryption system in circulation system in circulation.

- Generates public/private RSA keys.
- Encrypts messages to be transmitted using the destination’s public key
- Decrypts messages received using the recipients private key.
- Authentication messages with digital signatures
- Manages key rings that keep track of destination’s public keys.

The following is a simplified description of how PGP is used to send an e-mail message:

1. PGP creates a random session key for the message being sent.
2. PGP uses the IDEA private-key algorithm to encrypt the message with the session key.
3. PGP then uses the recipient public RSA key to RSA-encrypt the session key
4. PGP bundles the IDEA encrypted message and the RSA encrypted session key together.

PGP van examine a file content and make an intelligent guess as to the file extension required. Some of the standard file extension are as follows

- .txt is attached to files created by a text editor or word processor before the file is encrypted.
- .pgp is attached to an encrypted binary file. It is also used for key rings
- .asc is attached to an ASCII armored encrypted file.
- .bin is created when you use PGP key generate option.