Study of security aspects for Session Initiation Protocol (SIP)

Student's name : Fatimah muttashar khudhair

Abstract

The aim of this study is to describe the built-in or proposed safety mechanisms to be combined with the Session Initiation Protocol (SIP). SIP is used to initiate, modify, and terminate session multimedia over an IP network. This study is divided into two main sections, the first part describes the security mechanisms implemented in the SIP and the second part describes a number of proposed security mechanisms that can be implemented in the SIP.

Keywords

Session Initiation Protocol (SIP), Security Mechanisms, security aspects, User Agent (UA), Session Description Protocol (SDP);

1. Introduction

This chapter serves as an introduction to the rest of the topics. First, the background From the topic presented. After this is the section on the structure From the topic, give the reader an overview of the contents

1.1 SIP protocol definition

SIP (Session Initiation Protocol) as defined in IETF RFC 3261 is a multimedia signaling protocol used for multimedia session establishment, modification and termination. The session may be a voice session, a video telephony session, a chat session, a fax session, or whatever multimedia session.SIP is a text-based totally client-server protocol Looks like HTTP The cause for its maximum easy nature and flexible design; this protocol is becoming a maximum commonplace than the H.323 family of relatives of protocols . The SIP protocol is designed to be impartial of the underlying transport protocol, so SIP applications can run on TCP, UDP, or other lower-layer networking protocols .Considered this SIP is an application layer protocol.
Development Protocol SIP: 1996, uses UTF-8 encoding SIP , uses port 5060 both for UDP and TCP. SIP may use other transports SIP does not provide services. Rather, SIP provides primitives that can be used to implement different services.

1.2 Uses SIP

Typically, the SIP protocol is employed for
1.SIP is used for signaling and Management multimedia communication sessions in applications of Internet phone for video and voice calls, privately IP phone systems, in instant messaging over Internet Protocol (IP) networks also as mobile calling over (VoIP)
2. used for multimedia session establishment, modification and termination.
3. creating and terminating sessions with one or more participants.
4. interactive, multimedia communication sessions between users.
.Many Applications: VoIP Distributed Classroom Virtual Meeting Shared Whiteboard Publish-Subscribe based applications, etc...

1.3 What is SIP ?

SIP supports 5 aspects of creating and terminating multimedia connections: User location: determining the highest system that will be used for communication User availability: determining the willingness of the connected party to interact in communications User capabilities: setting media and media parameters to be used for session setup: "ringing", creating parameters Session in both call and invite session management: including moving and ending sessions, modifying session parameters, and calling services

1.3.1 Create a SIP session and end the call

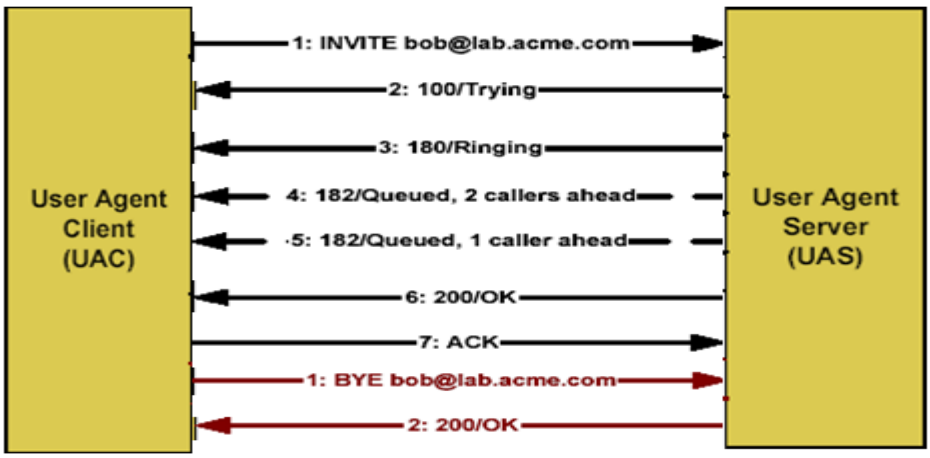

Figure 1 to Create a SIP session and end the call

1.3.2 SIP call forwarding

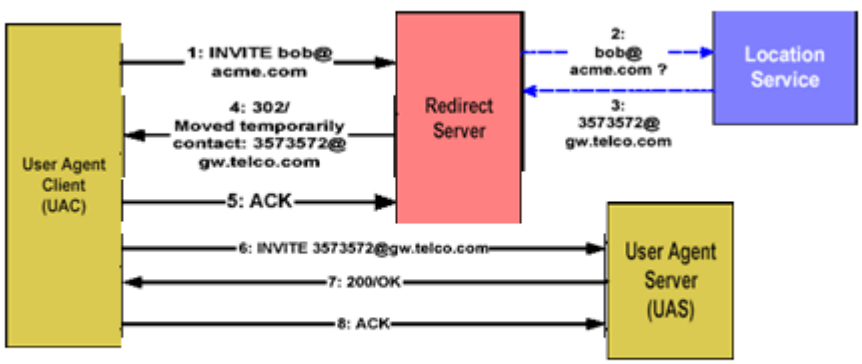

Figure 2 SIP call forwarding

1.3 . 3 Call Proxying

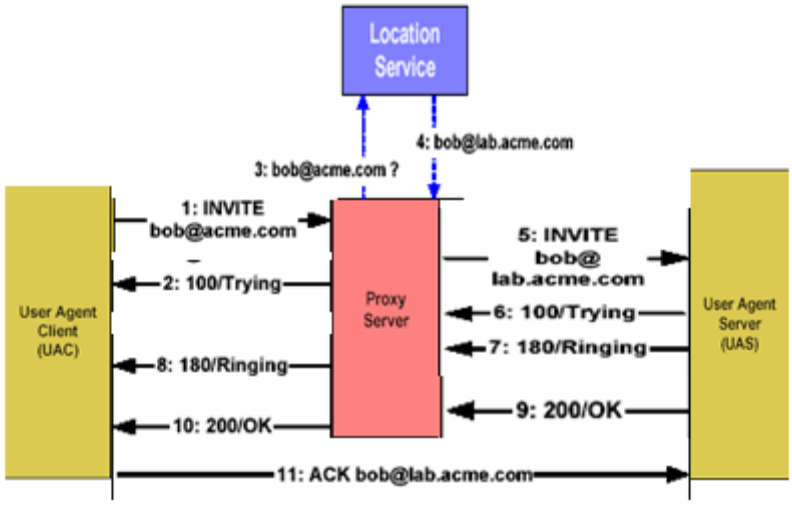

Figure 3 Call Proxying

2. security aspects

The section provides the reader with some relevant background information. And signals that may be necessary to understand Parts of the rest

2.1 Encryption targets

The main goal of encryption is to provide the following services:

1. Confidentiality
2. Authentication
3. Data integrity
4. Non-repudiation

Confidentiality: is a service used to keep information confidential for everyone Unauthorized to access it. Encryption is one way to provide confidentiality ,

Authentication :is a service used to identify information or entities The definition of information is often called the data authentication or data origin message Often called entity authentication and identification .Message authentication confirms to the recipient that the authorized party has created some information. Encrypted verification of information is often associated with that which proves that only the authorized entity will obtain it. Authentication of one entity enables one entity to verify the identity of another entity. A common way to verify this is by granting a type of grant to an organization, known and known and known, the judge Message authentication confirms to the recipient that the authorized party has created some information. Encrypted verification of information is often associated with that which proves that only the authorized entity will obtain it. Authentication of one entity enables one entity to verify the identity of another

entity. A common way to verify this is by granting a type of grant to an organization, known and known and known, the judge.

Data integrity: is a service to detect unauthorized manipulation of information. Manipulation includes insertion, deletion, and substitution. Secure Retail Functions It may be used to provide data integrity,

Non-repudiation : is a service that prevents the entity from rejecting the ex Commitments or actions. Digital signatures are one way to provide dissatisfaction.

2.2 Network Security

In recent years there has been a serious trend in the field of information technology Especially on the Internet. Almost all modern projects are interconnected They also have access to the Internet as well as their own local area network that employees use. Almost all staff work is done online Or a local network, for example to approve and distribute email. Thus, the requirement for fixed and security devices is an important upgrade a company. With regard to security, there are the following types of network attacks Recognized by [1]

1. **Description**: Receive a message for the person or process that does not have the content The cipher is connected.

2. Traffic Analysis: Displays the side traffic pattern. For the rebels Communication can be measured when it comes to reaching a particular goal Message algorithm or message timer sharing. A person can select several offline messages One sender and message length.

3. Masking: importing messages into a fraudulent network The fountain. One person can send a message that looks like this Send another source or an unverified message He was adopted.

4. Modify Content: Modify the content of the message, including Registration, cancellation, transfer and change.

5. Setting up the mouth: a scripted custom sequence Between the parties, including promotion, termination and reorganization.

6. Changing the Time: After passing or updating messages. For Internet connection You may prefer your traditional message to take advantage Delays messages to reduce connectivity. to me Offline calling can allow anyone to follow the old message.

7. Disclaimer: Delete a message with permission or refuse to call Source message .Security researchers have designed and designed many algorithms Protocols designed to protect one or more designated ones This type of attacks. Many, including many textbooks, are good Security areas that identify the most common and useful. This is one of them [1], the reader is given sufficient information about how different algorithms are Work protocols. The message ID can be used as a parameter to lock it with 3 points 6. Components 1 and 2 can be locked using encryption and digital signatures Protects element 7. The following section refers to a more detailed description Clause 6 relates to taking measures to protect you.

2.3 Re-attacks

An attack in which valid messages are repeated maliciously or fraudulently by the creator or by the unauthorized party is called a replay attack. Repeat attacks can be started to gain authorized access to the service or impersonate another body. Replay attacks pose a threat to almost every system that is used to messaging Affect the state of the system. For example, if an attacker is able to replay a valid request, in a client server system, the attacker may be able to delete A specific file on the server or change a password. It seems very easy to carry out a successful answer attack, but it must be taken into account That messages may be encrypted. This eliminates the ability of attackers to do so Read the content in restarted messages and he or she will not be able to predict The result of the replay attack. A skilled attacker may use motion analysis Predict the content in the message

.The following examples of repeated game attacks are mentioned in [1]:
• **Simple replay:** The attacker simply expects the message and replaces it Later.
• **Returnable**: The attacker can replay a timestamp message For a valid period of time.
• **Undetectable repetition**: The attacker expects the message Not reaching the destination. When the attacker replaces the message The receiver is valid and cannot find that another cause is authorized Entity sent it before.
• **Repeat unchanged:** The attacker replaces the message Back to sender. The attack is possible if a symmetric key is used Encrypt the message and the sender does not have the ability to discern If a message stems from it myself. To gain protection against replay attacks,
the following approaches may be Used:
• **Timestamps**: The entities always attach a timestamp to their messages The receiver only receives messages with a valid timestamp, that is Timestamp corresponds to a specific time interval. It is sensitive because the entities Need to sync clocks with a small deviation depending on Windows Time interval accuracy. This certainly applies to offline communication There the bodies cannot synchronize their clocks to each other for the duration Relatively long period of time.
• **Sequence Number:** Entities always include a sequence number in message. So the receiver knows what number the next message sequence is Should be valid and messages with smaller or larger ones The sequence number will be deleted. The problem with this method is this Each entity must remember the sequence number for each entity it will do communicate with. A less secure approach to this problem is to always Start with a specific serial number for each new session.
• Challenge / Response: One entity first sends a random number to another entity. then The entity requires that subsequent messages contain the correct random number value. The problem with this method is that it only works online communication. However, this method is preferred in client server applications The server responds to an invalid random number by sending a new response The generated random number is returned to the client. The client can then resend the message A new random number that the server considers valid. The important thing is Mention that the server should not use predictable old random numbers because Then we came back and we started.

2.4 Signalling

A signal is an exchange of information between communication components .You must provide service and maintain. This information Call forwarding, monitoring and termination between one or more callers. from On traditional phones, the caller is identified by a unique address Phone number. It is important to understand that there are no signals This includes actual data transfer between callers. Make transfer possible instead. Today, most signals are signalled through circuit-switched networks System Protocol 71 (SS7), a very flexible protocol with multiple protocols Feature. However, there is a more flexible and cost-effective way to search IP network, any IP phone. IP telephones can be installed Conversations can be exchanged between parties adapted to different data Media, ie data, audio, image, and video. Also adjustable Session during a call, ie change media type, add caller and remove caller Clearly flexible signals are needed to use all of these functions. There are many signal protocols on IP networks, most of them Recognized are the Session Initiation Protocol and H.323 [6].

2.5 SIP

The SIP Session Initiation Protocol, SIP, is a layered protocol for applications that already existed Internet Engineering Task Force (IETF) multimedia Control Working Group. It defines initiation, editing and elimination Interactive, multimedia sessions between users.SIP has added other protocol elements that are widely used The Internet. This is a text client-server protocol that is almost identical Hypertext Transport (HTTP [13]) and structure as text encoding Plans are obtained from the Simple Mail Transfer Protocol (SMTP [16]).This facilitates tracking and

understanding of the protocol structure As mentioned above, SIP messages have the same structure as messages HTTP, and at least after the request line or the status line Six header fields. There may be an associated message after the header field Body and type of body specified by some header fields. do it For HTTP and SMTP, SIP supports popular multipurpose Internet mail Detection of the content in the message body (MIME [9]). More likely The message body includes the session drive protocol (SDP [15])A message that describes the media transfer after the signaling step. MIME request contains P / SDP subtype for SDP message. Even if there is a SIP message In most cases the body may have an SDP message and may have a second MIME Subtypes, e.g. Text / plain or image / gif.
The client server structure is client-based, which allows for service. Sends the request The server processes the request and responds with the service. A Last SIP enabled device, SIP User Agent (UA) has both client and server Application. This is only natural if you are considering a phone that has both calls And accepts calls. All client requests in the UAE include a method in the request queue. Available There are six different ways in SIP [2]:

Method name	**Description**
INVITE	(Requests a session) Invites the serve UA r to a call and establishes new connection. It can contain media capabilities.
ACK	Final response to the INVITE
OPTIONS	Ask for server capabilities
CANCEL	Cancels a pending request
BYE	Terminates a session
REGISTER	Sends user's address to server

Table 1 Defined methods in SIP.

The UA response has the same structure as the HTTP response. All SIP responses contain a status line with an official description of the case number and reply to it. The position rules are grouped into six different chapters and each chapter shows a type of response. Most response header fields are copies of an independent response request. But there is a title that will be used for comment only. Comments can be message body and MIME type In most cases, this is the same as the corresponding application. UA Server may include an internal SDP message to discuss the type of media used when transferring media.
In addition to the UA client and UA server, other applications may process the SIP message as follows.
• Proxy servers
• Redirect to servers
• Registration servers
• Gates
The proxy server is assigned by sending the CA client request to the address specified in the SIP message. Proxy servers also have the ability to change parts of the header in a message, such as the Via field. They may also need to confirm the request before sending the message.
Answers from the UA server are also sent to the client. Answers are always the same as requests, that is, they are sent through intermediaries. If SIP UA is configured to always send its requests through a specific proxy, it is called an SIP UA proxy.
The reissue service does not make your request. After receiving the request, the server collects a list of alternative locations and returns the final response.

The registration server, also called the registry, is required to accept the REGISTER request from UA. The request includes information on how to get to UA.
Information is stored so that another UA may ask the registrar where the UA is. A registrar may require authentication.
Transitions between different types of networks are used, or if different protocols are used between networks. Transitions between SIP and H.323 are often used as examples.
For a detailed description of the SIP protocol.

3. The security mechanism of SIP

This section covers the current security mechanism standards . Because SIP is still under development, some security mechanisms are in place What is discussed in this section may be excluded in later versions.
There may also be new mechanisms added as standard in newer versions.

3.1 Authentication

Authentication ensures that the message is generated from a potential source This is a possible source I send. Authentication includes protection , Against modification, delay, iteration and redial .

SIP provides a stateless challenge-based authentication mechanism. The authentication mechanism is intended to be used in one direction only. But there is There is an opportunity for mutual acceptance, I am. Confirmation in both directions .Support for request and response integration is also supported.

The IETF SIP staff has not developed a new verification system, It uses almost the same authentication system as HTTP [3]. The difference is the definition of the protection domain in the HTTP case Identified by the realm,and the canonical root URL. The canonical root URL does that SIP not found, any files that can be retrieved, inserted or deleted as HTTP. And for The security domain specified by the realm,, userinfo, is the host and port Part URI Request.

3.2 Integrity

The order is only for authorized users You may not be able to edit a message unless a third-party edit is allowed ,Findings from authorized clients. Mostly anti-Semitism Only applies to certain parts of the thread. That is, without permission Fixed The problem with integrating protection in SIP is that messages are allowed Switching Internet servers. This means that it is Changes cannot be included in security protection.
The SIP standard defines how Pretty Good Privacy (PGP [10]) is used to get rid of it Signature clips are messages that have not changed web servers.
Signing is one of several ways to provide the integrity of the messages used Retail sales jobs. Even if it is a standard SIP document, please request comments (RFC) 2543, possibly a regular track with 'Draft Standard' mode [8] Be old fashioned and replace it with "draft-ietf-sip-rfc2543bis-0x" projects, Because x is the version number. Use PGP in current version, version 5 Signatures are excluded. Today, there is only very limited safety SIP protection provided by the feed identification system, Described in the first section. Although it is wrong to say that the SIP does not Supporting other security protection, the protocol makes no standard Determine how to do this. The above episode mentioned that there is no complete complete protection Message in SIP. But there are definitions of how to protect security S / MIME message, the text consists of media descriptions that may be interesting To protect from change. Although there is no complete integration protection for the message SIP, it is always possible to use the transport layer and network protocols it provides this feature. IETF SIP draft version 5 is recommended For SIP terminals that support TLS [4]. IP Security (IPSec [5]) is also a hot topic to provide protection for integration.3***2.3 Confidentiality***

Message confidentiality ensures that only authorized parties can read Content. In SIP, encryption is used to provide message confidentiality. In RFC 2543, there are two header fields, the encryption and response key,
It can be used for end-to-end encryption. There is also a definition How to use this header field for PGP encryption. As in the case of the message Security This identification is excluded in the following draft. President Fields that indicate encryption are excluded Scope is in SIP and can be moved to lower layers.
SIP encryption issue from SIP is this server network You must view specific sections of the message in order to access it The project. These parts can be sensitive to users, which means most of the things The benefits of using encryption are lost. There are also concerns about key exchange Because the end of the encryption algorithm depends on the shared keys By different users. SIP does not specify any key switching systems
Lower layer protocols like TLS and IPSec. The result is that it is not All end-to-end encryption support may be a future standard sip. Although not all passwords are encrypted, it is possible End of writing from S / MIME end

3.***4 Analysis***

The purpose of the following section is to give the reader an in-depth analysis of the security mechanisms in SIP. The analysis is based on the most recent draft of the SIP protocol [2] from the IETF.
Modern systems of cryptology may be able to protect against different types of security. But there are also other designs to consider when applying, for example. performance, power usage, user-friendliness, etc. SIPs will be deployed on many different platforms that will include some of the long journey times and the provision of sufficient power, for example. mobile phones. Complex maps that provide robust protection will not be possible in SIP. Building a new map based on demands and constraints is always possible but takes a long time to achieve. History shows that new maps always have serious security issues when they are first released for public use. Even though the base of the new map remains hidden, it does not prevent users from collecting for illegal creation. The IETF was clearly thinking about the requirements when it came to setting up a security framework for SIP but there is still very little work to be done. Thick only makes basic and Digest adjustments today, it is not enough to eliminate all security threats. The framework needs to be expanded to prevent security threats so that the attacker and listener can be heard.

4. Security mechanisms are proposed in SIP

This section describes the protocols or security systems you can share In the future it is either related to the SIP protocol or can be used with SIP Improve security. Most of these protocols or graphs are recommended
The proposal is not from the IETF, but some data are available Sitting down.

4.1 S / MIME

Multiplex Internet Mail Security (S / MIME [10]) is secure Expanded to the MIME standard.

4.1.1 MIME

MIME is a generic message sending format, which is embedded correctly in RFC 822. The main purpose of expanding this standard was to resolve a problem Distribute and coordinate different forms and files of national language icons, But there are other minority issues that can be resolved by MIME.
Applications need MIME support MIME, like SIP, should support the three header fields, described in Table

Header field	Description
MIME-Version	Its value must be “1.0”.
Content-Type	Describes the data in the body of the message and it should be specific enough, that the receiver can decide how to represent the data to the user. The content type may also be extended with one or several parameters.
Content-Transfer-Encoding	Specifies the type of transformation that has been applied to the data before it was sent, e.g. radix-64 or binary encoding.

Table 2 :MIME header fields.

SIP, as well as HTTP, is not allowed in the Content-Transfer-Encoding header field, but instead the Content-Encoding header field provides us with a smaller target. Both SIP and HTTP are "8bit-clear" transmission protocols and therefore these protocols do not require a clear Content-Transfer-Encoding header field. The Content-Encoding header field is used to specify deeper code, for example. compression. The Field Content-Type header field is the top most important MIME header and its values are organized into different content types. Any kind of content It is organized into different types. For SIP, the most important and most commonly used type of content is the type of application with SDP as the subtype, which means that the message data is SDP and other types of content and the types are rarely used, but sometimes ... the type of multi-segment content used. Multiple content types have more than one body of data in the message body, and each content type is separated by a weight limit. An example of using multiple content types in SIP is when a user wants to send an SDP message, but he also wants another user to see a caller image when invited.

4.1.2 S / MIME functions

S / Mime owns, encrypts, or records both MIME entities and encrypted ones. If both encryption and signature are required, default S / MIME attributes should be used. Depending on the situation, it may be best to save it first and then show it or vice versa.

To enable these capabilities, S / pantomime introduces some new types of new source-type mime, as shown in table 3, to different types of new mime content.

S/MIME entities	Description
multipart/signed	A multipart content type containing two parts. The first part can be of any MIME content type and the second part is the signature of the first part. The main reason to separate the signed data from the signature, is that entities, which do not support S/MIME, will be able to read the signed data. This functionality is often called clear-signing.
application/pkcs7-mime	A signed, encrypted S/MIME entity or just an entity that contains a public key certificate, depending on what parameter that has been specified for this content type.
application/pkcs7-signature	The content type of the second part in the multipart/signed content type, described above.
application/pkcs10-mime	Content type used for requesting a public key certificate from a certification authority.

Table 3 Entities defined in S/MIME.

4.1.2.1 MIME address encryption

In S / MIME, create a / pkcs7 mime application entity with the smime-type parameter of "enveloped-data" and provide an object containing MIME encryption, key sender, encryption algorithm used, and key session key By the MIME value. The following steps, borrowed from [1] and [10], describe how to create an S / MIME source in MIME encoded space.
1. Configure MIME locations as standard and individual MIME settings. The methodology is described in the MIME specification [9]. Type, type, price, description The S / MIME signature field includes, among other things, objects that contain a MIME signature field. .enveled-data S / MIME source contains objects, including others.
MIME is hidden somewhere. Simply-only S / MIME storage includes objects that are included only in public certificates.
2. Encryption A semi-random key is created for the encryption algorithm. Supported content is Triple DES and RC2 [14] with a 40-bit value. Guidelines for these issues can be found in [1].
3. Secure the segment key using the RSA algorithm and use the public key in the certificate key to the recipient.
4. Exit MIME with the selected solution and put the result in CMS type. An algorithm file used to hide MIME transactions, an algorithm used to hide session keys, key conferencing is used, and also contains distributor key credentials.
5. CMS object encoding using radix-64.
6. Connect the CMS encoded object to the / pkcs7-mime application. Each S / MIME supports Diffie-Hellman algorithm for key session design. Points 2 and 3 above are not included when using this method. Alternatively, an open key sequence is generated according to the Diffie-Hellman content consensus method described in RFC 2631 [12].
For example, from RFC 2633, for an S / MIME source with the MIME values shown in Figure 1

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V
```

Figure 4 Example of an encrypted MIME entity.

4.1.2.2 Signature of MIME entity

Signing a MIME entity in S / MIME is achieved by creating an application / pkcs7-mime entity using the smime-type parameter of "signed-data" and attaching an object containing the MIME entity signature . The sender's public key certificate, the algorithm used to encrypt the message digest, and the algorithm used to calculate the message digest. The following steps, borrowed from [1] and [10], describe how to construct an S / MIME entity containing a signed MIME entity.
1. Prepare a MIME entity according to the standardized rules and normalize the MIME entity. The

normalization procedure is described in the MIME specification [9]
2. Select the algorithm to use when calculating the message digest. Supported algorithms are MD5 and SHA-
3. Process the MIME entity with the selected algorithm and calculate the message digest.
4. Encrypt the message digest using the RSA algorithm and use the public key in the recipient's public key certificate.
5. Attach the encrypted message digest to the CMS object. The object also contains the algorithm used to calculate the message digest, the algorithm used to encrypt the message digest, the sender's public key certificate, and information about the signed content.
6. Encode the CMS object with radix-64. All S / MIME implementations support the Digital Signature Standard (DSS [13]), and if it is used, point 4 above is excluded. Instead, the signature is calculated
Uses the digital signature algorithm (DSA [13]). Public key
What is used to calculate the message digest from the signature is to be included in the public key certificate included in the CMS object.
RFC 2633 example, S / MIME entity consisting of signed MIME The entities are shown in Figure 2.

```
Content-Type: application/pkcs7-mime; smime-type=signed-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB9HG4VQbnj7
77n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBghyHhHUujhJhjH
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh
6YT64V0GhIGfHfQbnj75
```

Figure 5 Example of a signed MIME entity.

4.1.3 SIP S / MIME

The S / MIME usage suggestions for SIP correspond to the S / MIME description.[10] However, there are exceptions.
• Only multilateral / signed parties and S / MIME pkcs7-mime entities are supported by SIP messages.
• SIP M / SIME support agents should only support MIME signatures and S / MIME agencies with public key certificates. SIP UA can support hidden MIME agencies.
• Multipart / Signature must be used with separate signatures to suit S-MIME users.
S / MIME requires a behavioral component. Also, the cost of the cooking parameters should be "required".
• If the SIP UA key does not have the required public key certificate, it is not sent to secret MIME agencies. SIP UA may send an optional application to another SIP UA with a fixed profile to request a remote certificate.
• SIP UA must include S / MIME features and CMS mapping to facilitate future connections. SIP UA can encourage recipients to respond to signed authority from MIME, as defined by the CMS element.
• SIP UAs that support S / MIME SHA-1 must support at least as signature and Triple DES encryption algorithm. Signatures and other encryption algorithms can be supported.
Each MIME agency must be signed with one public key certificate. If SIP UA receives multiple entities signed by MIME, the last signature must be treated as the only public key certificate for this agency.

References

[1] William Stallings. “Cryptography and Network Security : Principles and Practice, Second Edition”. Prentice-Hall, June 1998.
[2] Rosenberg, Schulzrinne, Camarillo, Johnston, Peterson, Sparks, Handley, Schooler. “SIP : Session Initiation Protocol”. draft-ietf-sip-rfc2543bis-05. Internet Engineering Task Force, October 2001.
[3] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart. “HTTP Authentication : Basic and Digest Access Authentication”. Request For Comments 2617. Internet Engineering Task Force, June 1999.
[4] T. Dierks, C. Allen. “The TLS protocol version 1.0”. Request For Comments 2246. Internet Engineering Task Force, January 1999.
[5] S. Kent, R. Atkinson, “Security architecture fot the internet protocol”. Request For Comments 2401. Internet Engineering Task Force, November 1998.
[6] “ITU-T Recommendation H.323”. Draft v4. ITU-T, November 2000.
[7] M. Handley, V. Jacobson. “SDP : Session Description Protocol”, Request For Comments 2327. Internet Engineering Task Force, April 1998.
[8] S. Bradner, “The Internet Standard Process -- Revision 3”. Request For Comments 2026. Internet Engineering Task Force, October 1996.
[9] N. Borenstein, N. Freed. “MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies “. Request For Comments 1341. Internet Engineering Task Force, June 1992.
[10] B. Ramsdell. “S/MIME Version 3 Message Specification”. Request For Comments 2633. Internet Engineering Task Force, June 1999.
[11] J. Callas, L. Donnerhacke, H. Finney, R. Thayer, “Open PGP Message Format”. Request For Comments 2440. Internet Engineering Task Force, November 1998.
[12] E. Rescorla, “Diffie-Hellman Key Agreement Method”, Request For Comments 2631. Internet Engineering Task Force, June 1999.
[13] Arati Prabhakar, “DIGITAL SIGNATURE STANDARD (DSS)”, Federal Information Processing Standards Publication 186. National Institute of Standards and Technology, May 1994.
[14] R. Rivest, “A description of the RC2(r) Encryption Algorithm”, Internet Draft draft-rivest-rc2desc-00.txt, Internet Engineering Task Force, June 1997.