Journal of Intelligent Information Systems, Vol.9, No.2, November, 2003 (pp.39~50)

An Architecture for Certificate and Agent Based E-mailing to Block Spam Mail

SangZo Nam

Department of Management Information Systems, Mokwon University Daejeon, Doandong, Korea
(*namsz@mokwon.ac.kr*)

Deleting unsolicited email, popularly known as spam mail, is an annoying task for Internet users. Moreover, spam mail causes a variety of social problems. At present, legal restrictions cannot eradicate spam senders. As a result, many technical methods to eliminate spam mail such as spam filtering and online stamps have been introduced. However, the process of blocking spam mail can inadvertently result in suspension of indispensable or beneficial communication. In this paper, we propose a certificate and agent based emailing architecture that can block spam mail, while at the same time approve certified mail. This architecture can be accelerated by synergistic utilization of digital signature and electronic document interchange.

Key words: Certificate; Certificate authority; Spam mail

Received: October 2003 Accepted: November 2003 Corresponding Author: SangZo Nam

1. Introduction

Purpose of Study

In recent years, deleting spam mail has been an annoying everyday affair for most email users. Such spam mail is generally comprised of advertisements for obscene sites and push marketing mails. The major problem of obscene spam mail is that it is sent indiscriminately, and as such the receivers include both adults and children. Such mail often contains not only images of nude men and women, but also portrayals of sexual acts, rapes, bestiality, abnormal sexual behaviors, and so on. Exposure to such materials risks distorting people's healthy conception of sex. Other spam mails that contain no obscene or violent contents have the effect of causing people to avoid all push marketing mail. At present, legal restrictions cannot eradicate spam senders. Meanwhile, law-abiding companies undergo difficulties in promoting and marketing their products via push mails. Furthermore, through efforts to block spam mail, Internet users often lose

indispensable or beneficial communication. Even teachers who want to send e-mails to their students experience service denials from mail service providers due to restrictions of broadcast messages. In this paper, we propose a certificate and agent based emailing architecture that can block spam mail, while at the same time approve certified mail.

Anti-Spam Methods

In Korea, the current regulations state that push mails should contain the phrase of "advertisement" on the title together with a hyperlink of "refusal" to remove the email address from the mailing list[1]. However, spam mail usually violates this regulation. There are currently some technical methods to prevent spam mail as follows.

Spam filtering

Spam filtering is the most utilized method. The administrator or the user creates filtering settings such as mail addresses, IP addresses, domain names of spam senders, words or phrases in the title, etc. However, malignant spam senders do not follow regulations and frequently change their email addresses, domain names, and IP addresses. Therefore, some mail service providers adopt a negative filtering resolution, which accepts mail from pre-accepted senders only while other mail is sent to a bulk mailbox. Spam filtering, however, can inadvertently block law-abiding mail that contains the legal statement of "Advertisement".

Online stamp, IP address registration

Companies which want to send a certain quantity of broadcast mails to the receivers of a mail service provider that employs the strategy of an online stamp and/or IP address registration must register their IP addresses with the mail service provider. Companies must pay for the online stamps in proportion to the quantity. If the evaluation from the email receiver validates the mail, then the cost can be remitted[2]. This method requires real information of the sender, and can reduce spam mail by rejection of unregistered mail. From the view of advertisers, this is burdensome, as they incur large expenses for push advertisements. Therefore, only a few mail service providers have adopted online stamp systems[3][4]. Some mail service providers have adopted IP address registration only. However, if a malicious spam sender sends email within the prescribed limit, then it is impossible to block that mail.

Secure emailing approaches

Thus far, many approaches for secure emailing such as PGP[5], PEM[6], S/MIME[7][8][9], and PGP/MIME[10] have emerged. These protocols and techniques vary in many aspects such as acceptance of X.509 certificate, key authentication, algorithm, etc[11]. Furthermore, they are still evolving and face the task of integration and standardization. In this paper, we propose an architecture using a certificate and agent for the purpose of confirmation.

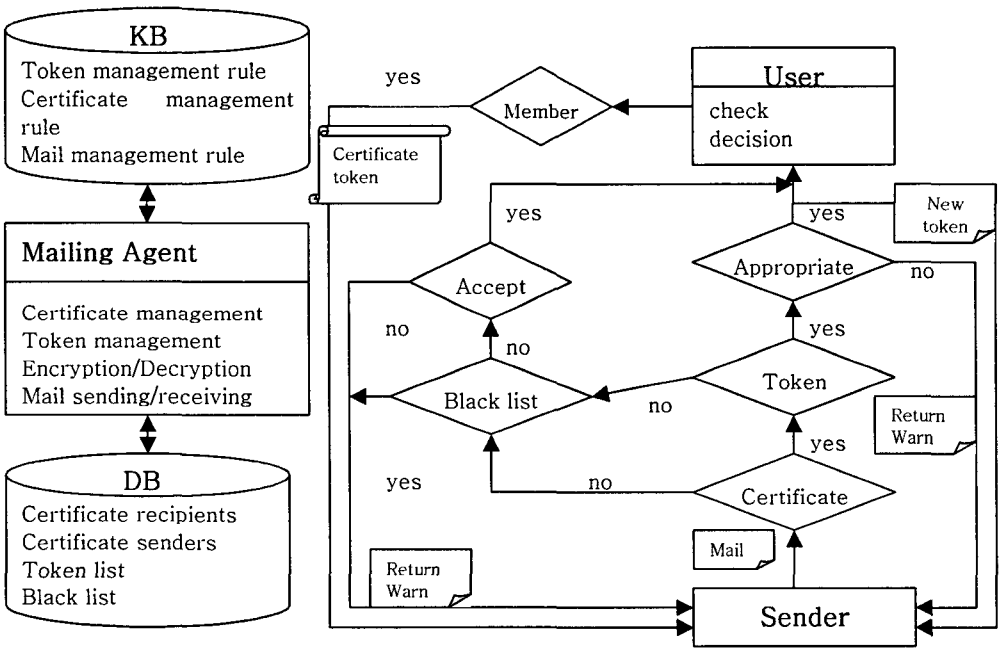

Figure 1. Mailing Agent

2. Proposed Architecture

Certificate and Agent

The contents which are to be included in the certificate are version, serial number, algorithm for digital signature, issuer, validity dates (start date, end date), subscriber, public key, restriction of certificate's usage, subscriber's power of attorney for a third party, occupational qualification, and fingerprint[12][13].

The registration authority, which is a subordinate of the official certificate authority, has to

inspect the subscriber's name, PIN, company name, company address, company telephone number, inscription number, etc[14].

When an individual becomes a member of a certain business site, then that person decides whether to receive push advertisement mails (advertisement-token: A-token) or whether to receive relevant/desired information only (information-token: I-token). According to the decision to receive mails, the customer's mailing agent creates a different token and sends it with the certificate to the business site. With the appropriate token and certificate, the company will send email encrypted by the customer's public key within the customer's certificate and customer's token with the company's certificate[15]. The customer's mailing agent manages the certificate and token using a knowledge base. Also, the mailing agent can determine whether it will transfer the incoming mail to the customer according to the policy of the certificate and token. After reading the email, the customer decides whether the email is useful and/or it contravenes the designated rules or regulations. If the mail from the company is problematic or undesirable in any way, then the customer can decide not to send the A-token to the company again. If the email is spam, then the sender will be included on a black list. In the case of acceptable mail, the user presses an "OK" button. Then the mailing agent will create a new token and send it to the company's mailing agent.

The token includes token type, issue time, expiration, recipient, fingerprint. The token cannot be modified due to the fingerprint and is digitally signed by the user's private key. The token is issued to the merchants only and is used once. Therefore, if a token is returned, then

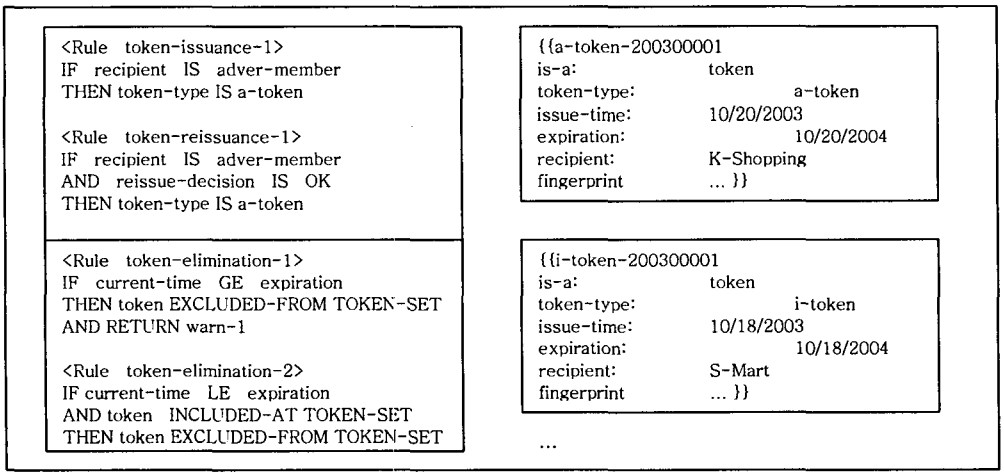

Figure 2. Illustrative Token Management Rules and Knowledge Base

the token is removed from the token list. The mailing agent will not accept an incoming token that has been removed from the token list. Therefore, a copied token cannot be used.

Knowledge Base

The knowledge base contains token management rules, certificate management rules, and mail management rules. The token management rule consists of rule- token-issuance, rule-token-reissuance, rule-token-distribution, rule-token-reception, rule-token-elimination, etc. The certificate management rule consists of rule-certificate-application, rule-certificate-distribution, rule-certificate-reception, rule-certificate-termination, rule-certificate-elimination, and so on. The mail management rule consists of rule-mail-sending, rule- mail-reception, etc.

An example of token management rules and a knowledge base is shown in Figure 2.

Circulation Architecture

There are two types of certificates, merchant and client certificates. All the communication parties are recommended to possess a certificate.

The mail can be classified in terms of the communicating parties as follows:

- peer to peer: an individual sends email to an individual; a token is not applied
- business to a customer who is a member and has agreed to receive advertisements
- business to a customer who is a member and has not agreed to receive advertisements
- business to a customer who is not a member

Peer to peer

In this case, the sender is required to use his or her certificate.

① Individuals can receive their own personal certificates from the CA after submitting their real information.

② If someone wants to send email to other people, then that individual sends a message and the sender's certificate.

③ The receiver has a choice whether to receive email that does not contain a certificate. Otherwise, traditional technologies such as spam filtering or an online stamp can be applied.

④ The receiver can reply to the sender using the public key in the sender's certificate with

the receiver s certificate. Or the receiver can forward the sender s email to another person with the sender s certificate and receiver s certificate.

⑤ Other individuals can reply to the receiver using the public key in the receiver's certificate with their own certificate, or they can reply to the sender using the public key in the sender's certificate with their own certificate

⑥ Once the peer receives the other person's certificate, they will be able to send email encrypted by the other person's public key.

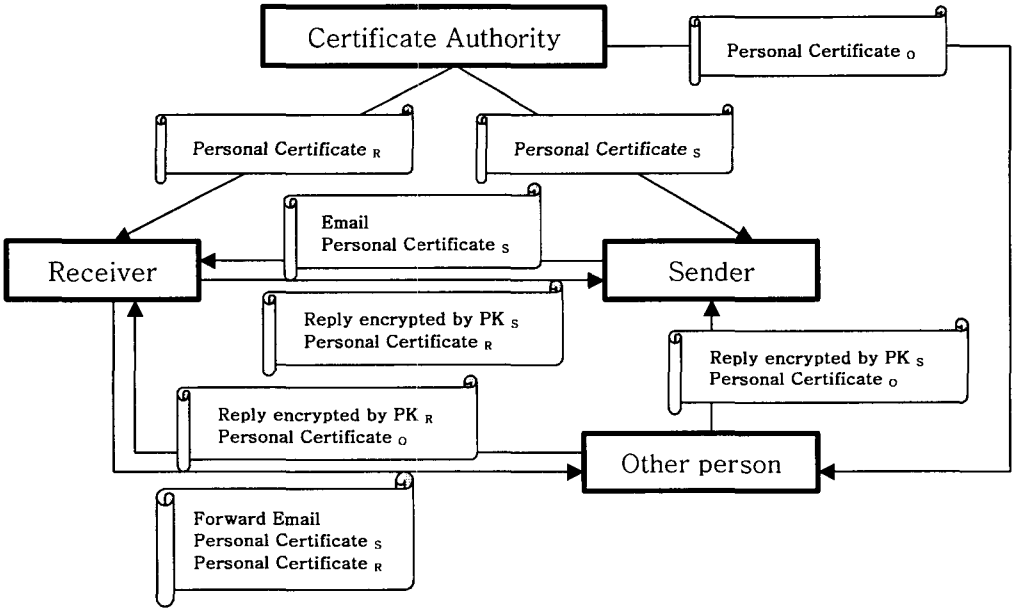

Figure 3. Architecture of Peer to Peer Certificate Based Emailing

Business to a customer who is a member of the business site and has agreed to receive advertisements

① Individuals receive their own personal certificates from the CA after submitting their real information. The merchant receives the business certificate from the CA after submitting their real information.

② The individual becomes a member of the merchant's site. The customer's mailing agent sends a personal certificate and a token that allows advertisements to be sent by the merchant (advertisement-token).

③ If the merchant wishes to send email to the customer, then the merchant's mailing agent sends a message encrypted by the public key of the customer, which has been sent within the customer's personal certificate together with the customer's A-token. Also, the merchant's mailing agent sends the merchant's business certificate to the customer.

④ The customer's mailing agent receives and decrypts email with the advertisement-token and certificate from the merchants. The token is removed from the token list. If the customer checks the email and assesses that it is useful, then he or she designates it as "OK". Then the customer's mailing agent sends another A-token to the merchant. Depending on the decision of the customer, the agent will send an advertisement-token, an information-token, or return the email with a warning and place it on a blacklist.

⑤ The customer can reply to the merchant using the public key in the merchant's business certificate with the customer's certificate. Or the customer can forward the merchant's email to another person with the merchant's certificate and customer's certificate.

⑥ Other people can reply to the customer using the public key in the customer's certificate with their own certificate, or they can reply to the merchant using the public key in the merchant's certificate. These individuals do not need to send their own certificate unless they are members of the merchant's site.

⑦ If the mail from the merchant is spam mail, then the customer can complain to the merchant. The customer can request to abandon his or her certificate. Furthermore, the customer can block the merchant's email. The merchant can be prosecuted according to their liability.

Business to a customer who is a member and has not agreed to receive advertisements

① Individuals receive their own personal certificates from the CA after submitting their real information. The merchant receives a business certificate from the CA after submitting their real information and being visited by CA

② The individual becomes a member of the merchant's site. The customer's mailing agent sends a personal certificate and an information-token to the merchant.

③ If the merchant wants to send relevant information email to the customer, then the merchant's mailing agent sends a message encrypted by the public key of the customer, which has been sent within the customer's personal certificate together with the I-token.

The merchant must be aware that they can send relevant information to the customer. The merchant also sends their business certificate to the customer.

④ The customer's mailing agent receives and decrypts email with the information-token and certificate from the merchants. The token is removed from the token list. If the customer checks the email and assesses that it is useful, then he or she designates it as "OK". Then the customer's mailing agent sends another I-token to the merchant. Depending on the decision of the customer, the agent will send an advertisement-token, information-token, or return the email with a warning and place it on a blacklist.

⑤ The customer can reply to the merchant using the public key in the merchant's business certificate with the customer's certificate. Or the customer can forward the merchant's email to another individual with the merchant's certificate and customer's certificate.

⑥ Other individuals can reply to the customer using the public key in the customer's certificate with their own certificate, or they can reply to the merchant using the public key in the merchant's certificate. These individuals do not need to send their own certificate unless they are members of the merchant's site.

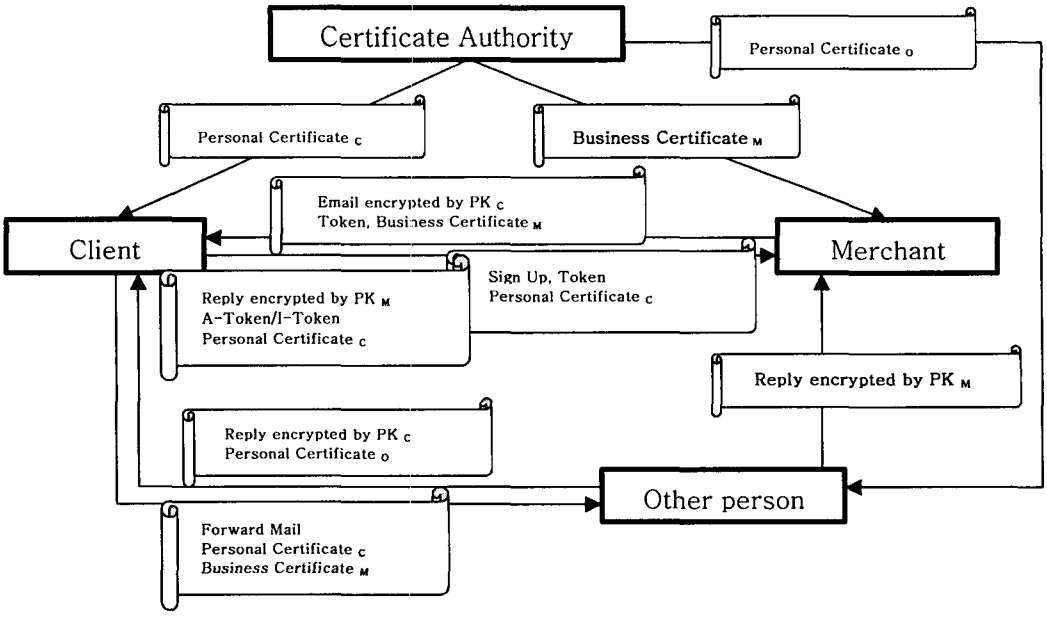

Figure 4. Architecture of Business to Customer with Token

⑦ If the mail from the merchant is spam mail, then the customer can complain to the merchant. The customer can request to abandon his or her certificate. Furthermore, the customer can restrict the merchant s email. The merchant can be prosecuted according to their liability.

Business to a customer who is not a member

① Individuals receive their own personal certificates from the CA after submitting their real information. The merchant receives a business certificate from the CA after submitting their real information.

② If the merchant wants to send email to any individual, the merchant should send the message with the merchant s business certificate.

③ An individual who receives email from the merchant has a choice whether to receive email which does not contain a certificate. Otherwise, traditional technologies such as spam filtering or an online stamp can be applied.

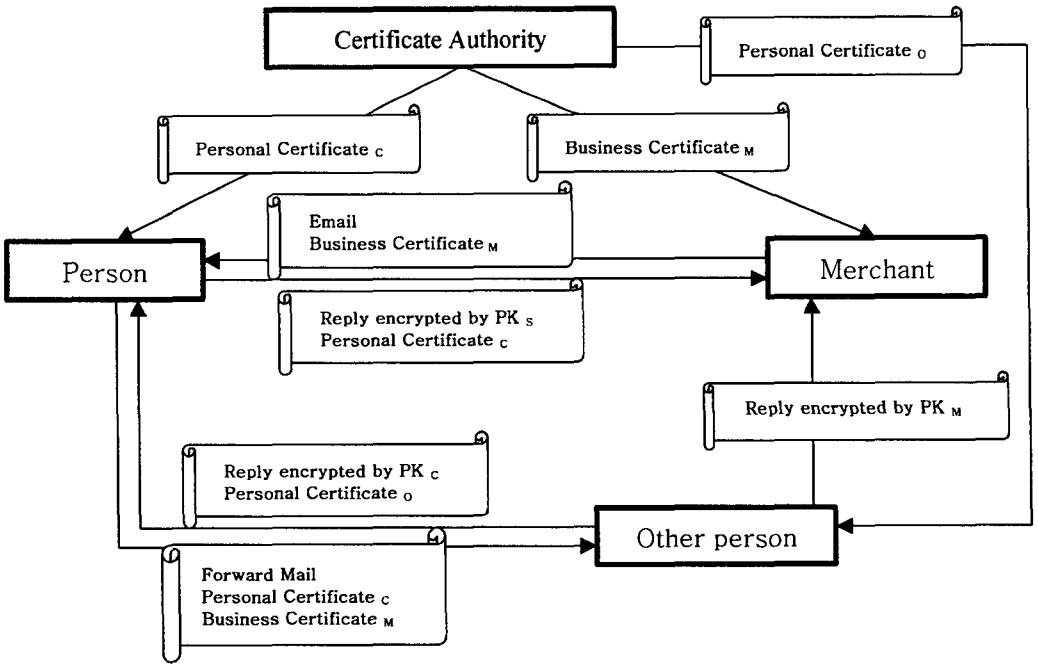

Figure 5. Architecture of Business to Customer who is not a Member

④ If the individual determines that the email offers interesting or useful information, then that individual can join the merchant's site. If the mail from the merchant is spam mail, then the individual can complain to the merchant. The individual can subsequently block the merchant's email and the merchant can be prosecuted according to their liability.

⑤ The individual can reply to the sender using the public key in the merchant s business certificate with the customer s certificate. Or the customer can forward the merchant s email to another person with the merchant s certificate and customer s certificate.

⑥ Other individuals can reply to the customer using the public key in the customer s certificate with their own certificate, or they can reply to the merchant using the public key in the merchant s certificate. These individuals do not need to send their own certificate unless they are members of the merchant's site.

Characteristics of Certificate and Agent-based Emailing

The characteristics of certificate based emailing are as follows:

- As an electronic document, the email can have legal validity.
- The merchant must reveal their real information, which is a critical restraint to criminals. Overseas server users who have enjoyed a legal way-out can be restricted.
- Irresponsible email can be reduced. This reduces unnecessary social costs incurred by spam mails.
- The private key and certificate can be saved in convenient media such as a smart card or USB key.

3. Conclusions

A certificate based emailing architecture advocates innocent communication, which requires real information of the participants. Such an approach might be considered contrary to the concept of freedom of expression. However, in order to avoid socially undesirable influences and consequences and to promote wholesome business opportunities, anonymity can be restricted. In the era of information, electronic documents have acquired legal validity through digital signatures within certificates. Cyber banking and cyber security trading have emphasized the importance of requiring certificates. In the near future, in most social activities on the Internet, such a certificate

will be essential. As such, certificate based emailing requires both analysis and preparatory steps. Many secure emailing protocols and techniques such as PEM, PGP, S/MIME, and PGP/MIME have been developed. The main focus of these approaches is security. In this paper, we proposed an architecture for certificate based emailing. We also adopted a mailing agent and token for the merchant in order to restrict spam mails, which have become a significant social problem. This architecture involves some costs, time, and inconvenience. Emailing service providers have not actively adopted secure emailing protocols due to such costs and inconvenience. However, in the near future, these hindrances can be overcome. Also, we hope our architecture to block spam mail can be integrated into the secure mailing protocol.

References

[1] Jung, J. W. (2000). "A Proposal for Settlement of the Legal Problems on the Spam E Mail," *Journal of Korea Commercial Law*, Vol. 19, No. 2, pp. 311-357.

[2] http://hmm4.daum.net/stamp/index.html.

[3] http://mail.nate.com/help/whiteip/whiteip.html?act=registration.

[4] http://realip.naver.com/realip.py/main.

[5] Callas, J., Donnerhacke, L., Finney, H., and Thayer, R. (1998). "OpenPGP Message Format," RFC 2440.

[6] Linn, J. (1993). "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures," RFC 1421.

[7] Lindberg, G. (1999). "Anti-Spam Recommendations for SMTP MTAs, BCP 30," RFC 2505.

[8] Freed, N., and Borenstein N. (1996). "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies," RFC 2045.

[9] Hoffman, P. (1999). "Enhanced Security Services for S/MIME," RFC 2634.

[10] Elkins, M. (1996). "MIME Security With Pretty Good Privacy (PGP)," RFC 2015.

[11] O'Mahony, D., Peirce, M., and Tewari, H. (1997). *Electronic Payment System*, Artec House.

[12] Housley, R., and Hoffman, P. (1999). "Internet X.509 Public Key Infrastructure. Operational Protocols: FTP and HTTP," RFC 2585.

[13] Housley, R., Ford, W., Polk, W., and Solo, D. (2002). "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC 3280.

[14] Kim, S. Y., Choi, B. K., Nam, S. Z., and Kim, B. H.. (2003). *Introduction to Electronic*

Commerce, Seoul, HongReong Science Pub.

[15] Pinkas, D., Ross, J., and Pope, N. (2001). "Electronic Signature Formats for long term electronic signatures, RFC 3126.