Compare and contrast the nature of certificates in PGP and S/MIME. Explain the web of trust made from certificates in PGP and in S/MIME.

Sanket Mundra, Harsh Bajaj, Raunak Rathour, Utkarsh Priyam, Prateek Mishra

V Semester B.Tech, Department of Information Technology,

IIIT-Allahabad,Prayagraj, India

Abstract: In this paper, we describe the nature of certificates in the PGP and S/MIME protocols and compare the trust establishment in both protocols.

I. INTRODUCTION

SMTP, Simple Mail Transfer Protocol was first developed in 1982. It had very few security features. Therefore to include features to digitally sign, encrypt, and decrypt emails 2 new standards were developed , PGP and SMIME.
The PGP (Pretty Good Privacy) and S/MIME (Secure Multipurpose Internet Mail Extensions) are the security protocols designed to serve for securing the electronic mail facility.They were introduced to add encryption/decryption and signature/verification features to SMTP (simple mail transfer protocol).

II. NATURE OF CERTIFICATES

In PGP, one user has the ability to give directly a public key to another user.
PGP does not mandate a policy for creating trust and hence each user is free to decide the length of trust in the received keys.
PGP was originated to address the security concerns of plain email or text messages.

In SMIME, the sender or receiver does not rely on exchanging keys in advance and share a common certifier on which both can rely. The user first obtains a public-private key pair from a centralized trusted authority. The private key is kept secret with the user and the public key can be distributed with others.

The nature of certificates
PGP certificates are similar to X.509 certificates, but the catch is that there is no need for a CA to sign these certificates, anyone can sign the certificates.
PGP certificates don't depend on the hierarchical level of trust.

X/MIME uses X.509 version 3 certificates which are signed by a CA.

These certificates are based on the hierarchical level of trust.

III. WEB of Trust

In cryptography, a web of trust is a concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a

hierarchy of such). As with computer networks, there are many independent webs of trust, and any user (through their identity certificate) can be a part of, and a link between, multiple webs.[1]

PGP:

In PGP, users exchange certificates or key rings for building trust between the users. Every user updates their public key ring table, when a new entity tries to communicate, according to their prior connections. Therefore, the trust values range from fully, partially to none.

Let's say this is Alice's public key table at this moment.

User ID	*Key ID*	*Public key*	*Prod. trust*	*Certificate*	*Cert. trust*	*Key legit.*	*Time-stamp*
Alice...	AB...	AB.....	F			F	.....
Bob...	12...	12.....	F			F	.....
Ted...	48...	48.....	F	Bob's	F	F	.....

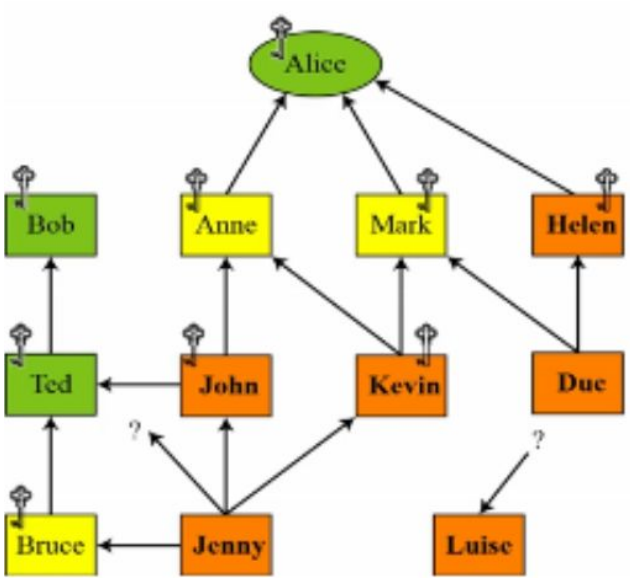
Now Anne wants to communicate with Alice, she sends her certificate to Alice.
Now, Anne's certificate is signed by Bob and Alice trusts Bob. Therefore Anne's entry has Certificate trust as full and key legitimacy as full, but since Alice has herself not communicated with Alice, therefore the producer's trust is partial.

User ID	*Key ID*	*Public key*	*Prod. trust*	*Certificate*	*Cert. trust*	*Key legit.*	*Time-stamp*
Alice...	AB...	AB.....	F			F	.....
Bob...	12...	12.....	F			F	.....
Ted...	48...	48.....	F	Bob's	F	F	.....
Anne...	71...	71.....	P	Bob's	F	F	.....

Now, John wants to communicate with Alice, he sends his certificate to Alice.
Now, John's certificate is signed by Anne and Alice partially trusts Anne. Therefore, Anne's entry has Certificate trust as partial and key legitimacy as partial, but since Alice has herself not communicated with neither Anne nor John, therefore the producer's trust is none.

User ID	*Key ID*	*Public key*	*Prod. Trust*	*Certificate*	*Cert. trust*	*Key legit.*	*Time-stamp*
Alice...	AB...	AB.....	F			F	.....
Bob...	12...	12.....	F			F	.....
Ted...	48...	48.....	F	Bob's	F	F	.....
Anne...	71...	71.....	P	Bob's	F	F	.....
John...	31...	31.....	N	Anne's	P	P	.....

Web of trust



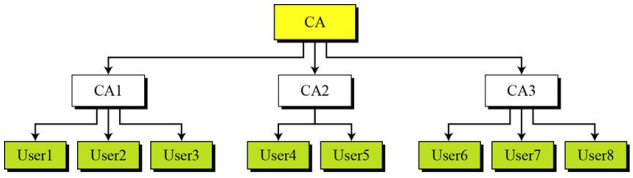
The key legitimacy is checked by assigning values to the Producer's trust (F = 1, P = 0.5, N = 0 or similar), and setting a threshold for each member yet encountered.

S/MIME:

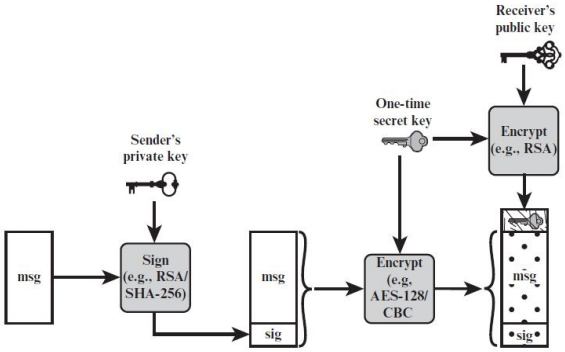
The email has to be signed with the sender private key and then the signature and the message are encrypted using a one time secret key. This one time secret key is encrypted with the receiver's public key. Then, only the recipient would be able to get the one time secret key to decrypt the secret message and verify the sender after decrypting the message with the recipient's private key. And, at the same time, no one else other than the sender would be able to modify the original message.

Web of trust

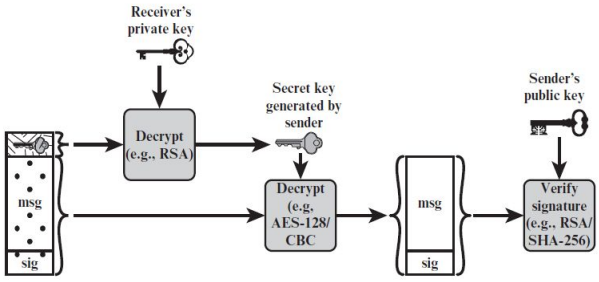
It relies on a hierarchically valid certificate for key exchange.



IV. S/MIME Protocol



The email has to be signed with the sender's private key (using RSA etc) and encrypted with a one time key which is further encrypted using the receiver's public key. Then only the recipient would be able to read the secret message after decrypting.



After that recipient decrypts the message with the recipient's private key. And, at the same time, no one else other than the sender would be able to modify the original message.

V. CONCLUSION

We learnt the differences in the nature of certificates between PGP and S/MIME and how these different protocols can be useful for different requirements like that of a Centralised network vs a non centralised network . We also learnt the trust Web of PGP and S/MIME with the help of an example and how trust can be an important factor in communication.

VI. REFERENCES

[1]https://en.wikipedia.org/wiki/Web_of_trust

[2] Video lectures.

[3]https://techdifferences.com/difference-between-pgp-and-s-mime.html