# 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.

**Group 26**
Sanket Mundra - IIT2018189
Harsh Bajaj - IIT2018190
Raunak Rathour - IIT2018196
Utkarsh Priyam - IIT2018197
Prateek Mishra - IIT2018199

# INTRO|_

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).

# PGP (Pretty Good Privacy)

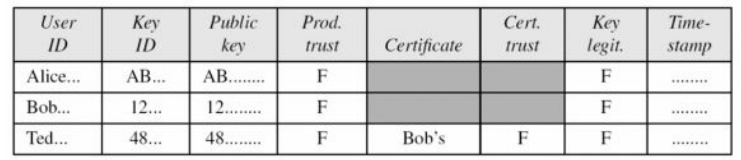
In PGP, one user has the ability to give directly a public key to another user.

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 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 understand this with an example.

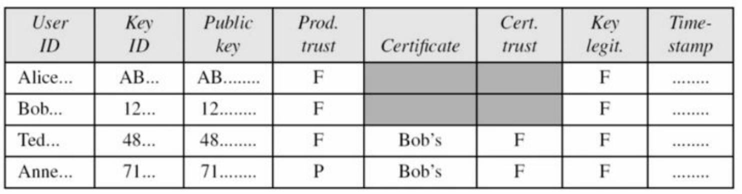
# PGP contd.



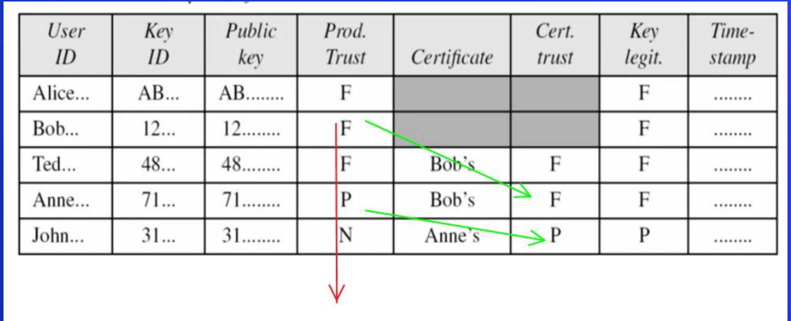
| User ID | Key ID | Public key | Prod. trust | Certificate | Cert. trust | Key legit. | Time-stamp |
|---|---|---|---|---|---|---|---|
| Alice... | AB... | AB........ | F | | | F | ........ |
| Bob... | 12... | 12........ | F | | | F | ........ |
| Ted... | 48... | 48........ | F | Bob's | F | F | ........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

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

Now Anne wants to communicate with Alice , it sends it 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



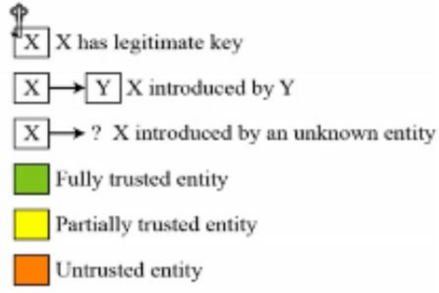
| User ID | Key ID | Public key | Prod. trust | Certificate | Cert. trust | Key legit. | Time-stamp |
|---|---|---|---|---|---|---|---|
| Alice... | AB... | AB........ | F | | | F | ........ |
| Bob... | 12... | 12........ | F | | | F | ........ |
| Ted... | 48... | 48........ | F | Bob's | F | F | ........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

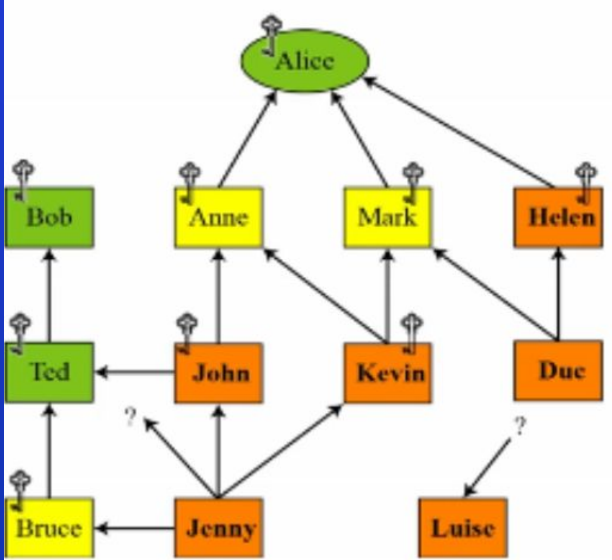


| User ID | Key ID | Public key | Prod. Trust | Certificate | Cert. trust | Key legit. | Time-stamp |
|---|---|---|---|---|---|---|---|
| Alice... | AB... | AB........ | F | | | F | ........ |
| Bob... | 12... | 12........ | F | | | F | ........ |
| Ted... | 48... | 48........ | F | Bob's | F | F | ........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

Now John wants to communicate with Alice , it sends it 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

# PGP web of trust





This is the web of trust of Alice, all of the other members in the network have their own web of trust.

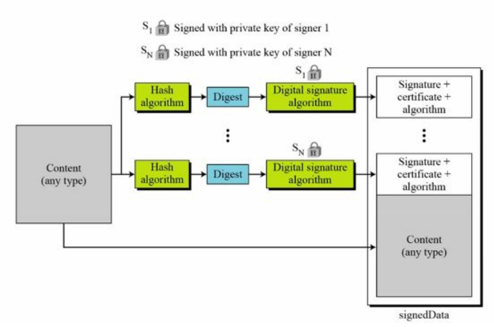
**We observe that Bob and Ted are fully trusted. But Anne Mark ,John, Kevin, Helen ,and Bruce all are understood to have a legitimate key. Why?**

Let's say score of a F-trusted Producer is 1 , for P it is 0.5 for N it is 0.And let the threshold be 1.

Now Bob, Ted and Alice (herself) all are fully known to Alice , now Anne has communicated with Alice therefore her score is 1. Since 1>=1 , therefore Alice has a legitimate key. Similarly for Mark and Helen.
Let's consider John, John has communicated with Ted and Anne therefore, its score is 1+ 0.5 which is above threshold. And so on.

# S-MIME(Secure Internet Mail Extensions)

...is a protocol that uses Public Key Cryptography to digitally sign, encrypt or decrypt emails. The sender or receiver does not rely on exchanging keys in advance and share a common certifier on which both can rely.

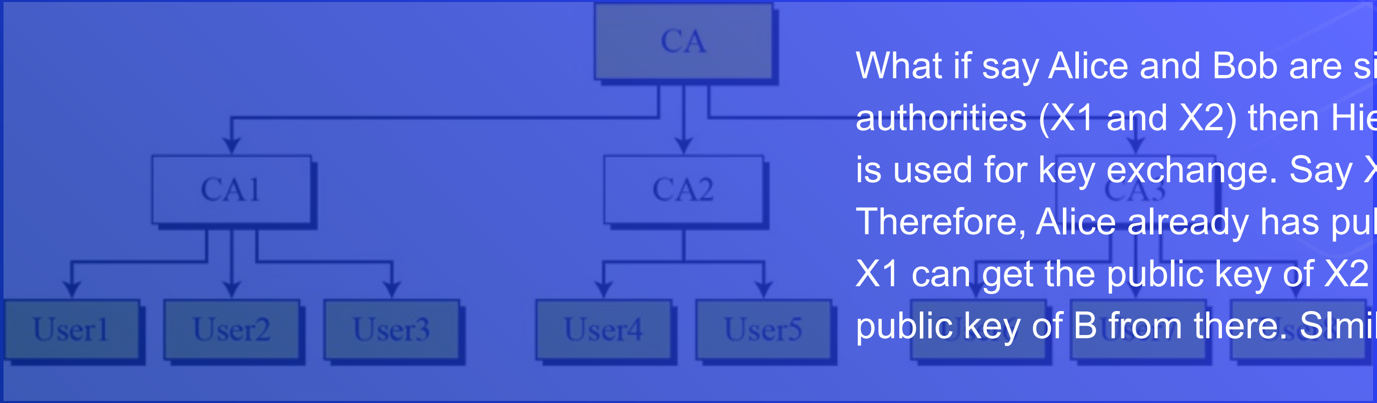

$S_1$ Signed with private key of signer 1
$S_N$ Signed with private key of signer N
Content (any type)
Hash algorithm
Digest
$S_1$
Digital signature algorithm
Signature + certificate + algorithm
Hash algorithm
Digest
$S_N$
Digital signature algorithm
Signature + certificate + algorithm
Content (any type)
signedData

Signed data content type

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.

# S-MIME contd.

The email has to be signed with the sender's private key and encrypted with the receiver's public key.  Then only the recipient would be able to read the secret message 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.



What if say Alice and Bob are signed with different signature authorities (X1 and X2) then Hierarchically validated certifier is used for key exchange. Say X1 and X2 is signed by CA . Therefore, Alice already has public key of X1 and therefore X1 can get the public key of X2 from there and then it can get public key of B from there. SImilar process for Bob.

# S-MIME vs PGP

| | |
|---|---|
| In S-MIME users communicate with fully trusted members. | In PGP every user has different level of trust over other users, and can set a trust threshold to communicate. |
| It is used for plain text only | Can also be used with multimedia files. |
| Hierarchically validated certifier | Key exchange with every other member in the network |
| Decentralised. | Centralised |

# Nature of Certificates

## PGP

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.

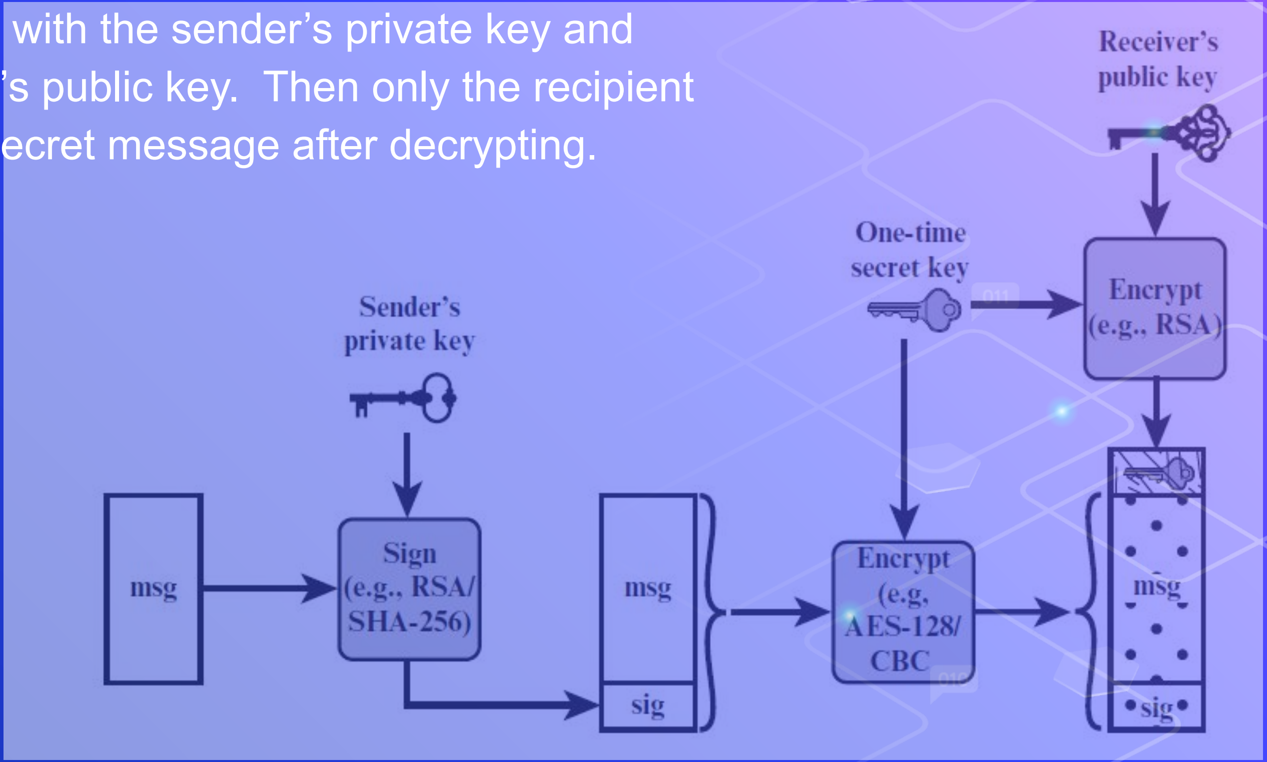
## S/MIME

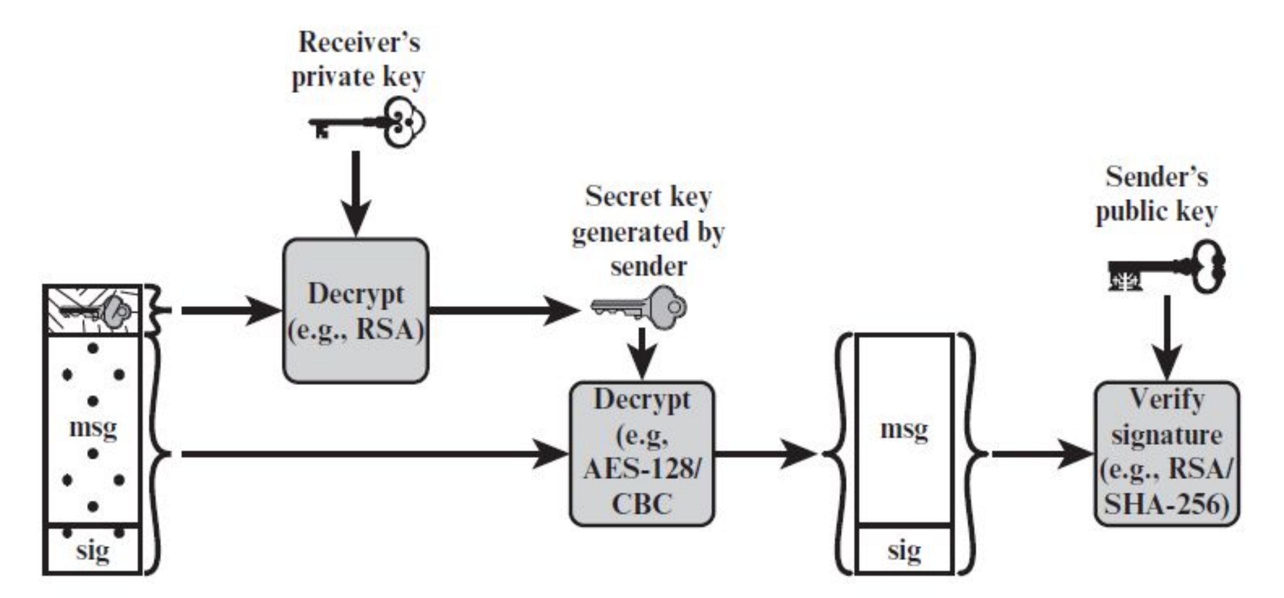
X/MIME uses X.509 version 3 certificates which are signed by a CA.

These certificates are based on the hierarchical level of trust.

# S-MIME protocol

The email has to be signed with the sender's private key and encrypted with the receiver's public key.  Then only the recipient would be able to read the secret message after decrypting.




Receiver's private key
Decrypt (e.g., RSA)
Secret key generated by sender
Sender's public key
msg
sig
Decrypt (e.g, AES-128/ CBC
msg
sig
Verify signature (e.g., RSA/ SHA-256)

After that recipient the 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.

# Thanks!