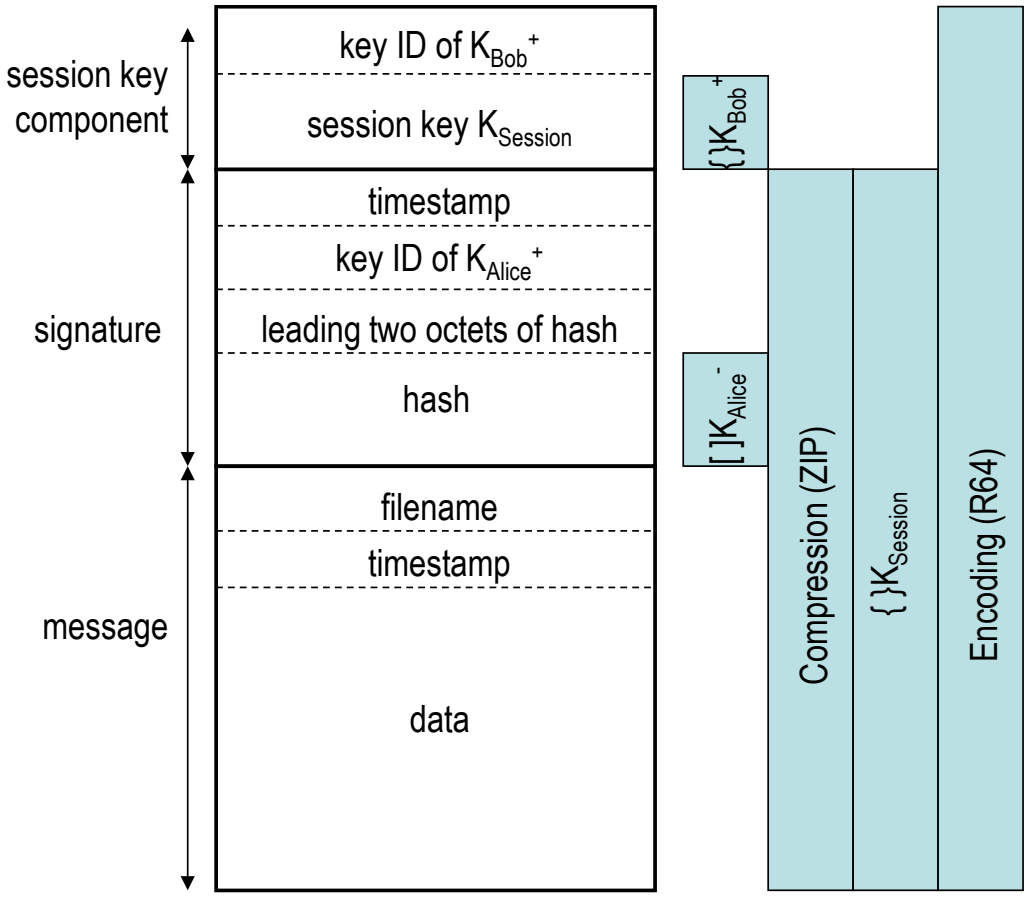
IK2206 – Internet Security and Privacy
Chapter 22 – PGP

22.1 Introduction (READ)

22.2 Overview (READ)

Following steps are necessary if Alice wants to send a PGP-encrypted message to Bob. It is assumed that the sender (Alice) has already generated a session key $K_{Session}$ in advance. The parts of compression and encoding are not further being cared about. Step 1 (encryption of the session key) can be sneaked in between step 4 and 5.

Step 1: Encrypt $K_{Session}$ using Bob's public key -> $\{K_{Session}\}K_{Bob}^{+}$
Step 2: Hash message → hash(message)
Step 3: Sign hash(message) with Alice's private key → $[hash(message)]_{K\text{-}Alice}$
Step 4: Encrypt message together with the signed hash of the messge $[hash(message)]_{K\text{-}Alice}$ using session $K_{Session}$ → $\{M \mid [hash(message)]_{K\text{-}Alice}\}K_{Session}$
Step 5: Send $\{M \mid [hash(message)]_{K\text{-}Alice}\}K_{Session}$ together with $\{K_{Session}\}K_{Bob}^{+}$ to Bob



Derived from: www.hit.bme.hu/~buttyan/.../PGP_SMIME.ppt

22.3 Key Distribution (READ)

- How are certificates organized in PGP?

  PGP doesn't require certificates at all, though they can make life simpler. People publish their PGP fingerprints (cryptographic hashes of public keys) on their web sites, on their business cards etc. Certificates are optional in PGP

- How is trust established, given that there is no central CA?

  Anyone can issue a certificate to anyone else. And users decide whose certificates they are willing to trust in authentication someone. PGP supports a trust model of anarchy.

- What are the different ways of determining the trustworthiness of a key?

  There is no defined way to find out about the trustworthiness of keys. It is best if one knows each other personally. **(???)**

22.4 Efficient Encoding (READ BRIEFLY)

22.5 Certificate and Key Revocation (READ)

- How are keys and revocations distributed?

  My key can only be revoked by me. The idea is that I will issue a key revocation only when I think someone has discovered my private key.

  I'll presumably generate a new key for myself, and distribute the key revocation for the old key as widely as possible.

22.6 Signature Types (READ BRIEFLY)

22.7 Your Private Key (READ)

22.8 Key Rings (READ)

- What is a Key Ring?

  Is a data structure which contains some public keys, some information about people, and some certificates. Usually this information is just stored locally.

- How is trust assigned to keys in the key ring?

  PGP allows you to assert how much trust you place on different people. There are three levels of trust: nonce, partial, or complete.

- Consider if the number of levels of trust is sufficient?
- For partial trust, the user may be able to assign a weight. Consider how such a weight could be computed.

22.9 Anomalies (READ BRIEFLY)

22.10 Object Formats (READ BRIEFLY)

You should have an idea of what the different objects are in PGP, but you do not need to study the details.