Key Encapsulation: A Public Key Encryption-Based Alternative to Key Wrap and Key Blocks

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT SCD LTD

1 Why use mixed/hybrid ciphers (asymmetric and symmetric ciphers) for key transportation?

Using public key encryption alone can be problematic. Public key ciphers are based on the mathematical properties of prime numbers or equivalent algebraic structures. Therefore, they are vulnerable to attacks based on the mathematical properties of these structures, while symmetric ciphers are not.

In public key encryption, the encryption of related messages may be itself related.
That is why mixed or “hybrid" schemes have been developed for key transportation.

2 First Generic Hybrid Key Cipher

Historically, a two-layer system using both asymmetric and symmetric keys has been developed to address these limitations:

- Symmetric methods can provide integrity protection
- Symmetric keys are unrelated, they avoid mathematical properties

This two-layers system is used in many norms, such as S/MIME for instance.
It works as follows:

1. Generate a symmetric key **K** using a specific algorithm (usually a key derivation algorithm)
2. Cipher a message M (a key in case of a key wrap scenario) with **K**: C= S-ENC (M, **K**) where S-ENC is a symmetric cipher algorithm compliant with the key **K**
3. Use the public key KEK|pub of the recipient to cipher **K: Kc**= AS-ENC (**K**,KEK|pub) where AS-ENC is an asymmetric cipher algorithm compliant with the key KEK|pub
4. Finally, output **Kc** and C

To recreate the message M (to get the value of transported key in a key wrap scenario), the receiving party will simply have to decipher **Kc** to get K using their KEK private key, KEK|priv:

1. **K**= AS-ENC (**Kc**,KEK|priv)
2. And finally decipher C using **K**: M= S-ENC (C, **K**)

This key wrap is still unsatisfactory. It is because it is proven that the ciphering of the symmetric key provides so much more security. In this scenario, we transport a key that is ciphered by another key, which is symmetrical and transported by public key encryption. This last operation is still vulnerable and limited, as per the original comments.

3 Key Encapsulation

To provide a mature key transportation algorithm based on public key encryption, the key encapsulation algorithm was designed. Its origins stem mainly from the work of cryptographer Victor Shoup.

The principle of the key encapsulation algorithm is slightly different from the initial 'two-layers' model. Key encapsulation still relies on both symmetric and asymmetric ciphers, but uses them differently.

In order to transport a key, K from a sending party (the "sender") to a receiving party (the "receiver"), a key generation algorithm is used as follows:

1. Generate a (ideally large) number **u** using a random number generator
2. Cipher **u** using the recipient's public key (K|pub) **c**= AS-ENC (**u**,K|pub), where AS-ENC is an asymmetric cipher algorithm compliant with the key K|pub
3. In parallel, derive a key, KEK, from **u** having the adequate length L . This is typically achieved by using a key derivation function KDF.

   KEK= KDF(**u**,L)
4. Wrap K using the key KEK and a specific key wrapping scheme (typically ciphering it with the key KEK using a symmetric cipher)

   K'=Wrap(K,KEK)
5. The last step is to concatenate the wrapped data K' together with c.
6. The sender outputs {K' | c} to the receiver.

The method's strategy is to use a key derivation function common to the sender and the receiver to generate the key encryption key, which is the base of the wrapping. The receiver deciphers **c** and gets **u** using their private key (K|priv): **u**= AS-ENC (**c**,K|priv)
With the knowledge of **u**, the receiver can get the KEK key and finally unwrap K' to get the key material K.

4 Conclusion

Key encapsulation mechanisms (KEM) are powerful alternatives to key blocks and key wraps. They combine symmetric and asymmetric ciphering in what is called 'generic hybrid ciphers' to provide the 'best of both worlds' and deliver maximum security for key transportation. Such KEM methods are described in the norm ISO/IEC 18033-2.