In chapter five under “Protecting Encryption Keys Used by Applications” the authors describe using a key-encrypting key to encrypt “…the actual key used to encrypt and decrypt data…”.

How would this work securely without someone using the key-encrypting key to decrypt the actual key and then decrypt the application data?