AES Key — Encoded in the Machine Readable Zone of a European ePassport

Author: S. Hick

December 2011
An AES encrypted message has been forwarded to you (CBC mode with zero initialization vector and 01-00 padding). Additionally, you have received the corresponding key – unfortunately not quite complete – in a form like a machine readable zone (MRZ) on an identity document as it is used e.g. with ePassports in Europe.

123456789<<<<1110182<<<<111116<<<<4
It is the objective to find the plaintext of the following base64-encoded message.

9MgYwmuPrjiecPMx61O6zluy3MtIXQQ0E59T3xB6u0Gyf1gYs2i3K9Jxaa0zj4gT MazJuApwd6+jdyel5iGHvhQyDHGVIAuYTgJrbFDrfB22Fpi2NfNnWFBTXyf7SDI
For encryption a key $K_{ENC}$ based on the Basic Access Control (BAC) protocol has been generated and applied. For decryption the following characters have been transmitted from which $K_{ENC}$ can be derived (The kind of coding of these characters is described in [1]):

12345678<8<<<1110182<111116?<<<<<<<<<<<4

Unfortunately, during transmission a character was lost and has been highlighted with a “?” . Nevertheless, you can make it visible again with the help of [2]. To be able to compute the key $K_{ENC}$ afterwards you can find an overview of the applied encoding protocols in [3], [4] and an example in [5].

The AES-encrypted message contains a code word that is to be entered as the solution.
You might benefit from CrypTool 1.4.30 for the cryptographic operations. Decode the base64 code before decryption (e.g. in CrypTool 1.4.30 with the function "Base64 Decode").
References

The following documents are available online at:

http://www2.icao.int

[1] ICAO MRTD DOC 9303 Part 1 Vol 1, p. IV-16 (Data structure of the lower machine readable line) and p. IV-42

[2] ICAO MRTD DOC 9303 Part 1 Vol 1, p. IV-24 to IV-26 (Check digits in the machine readable zone)

