Notice Bulletin No. 22
July 2018

EMVCo Annual RSA Key Lengths Assessment

In accordance with the Certification Authority Public Key management principles and policies set forth in section 10 of the *EMV Integrated Circuit Card Specifications for Payment Systems Book 2*, the payment systems will endeavor to synchronize the lengths and expiry dates of their Certification Authority Public Keys. EMVCo has completed its annual review of the Certification Authority Public Key lengths and expiry dates and has agreed on the following recommendations to the payment systems:

- 1408-bit keys are recommended to have an expiry date of 31 December 2024. Special portfolios that use a 1408-bit key should only continue to do so until 31 December 2025. Public keys that support these portfolios will need to remain in terminals until this date.
- 1984-bit keys are recommended to have an anticipated lifetime[1] to at least 31 December 2028.

In accordance with the principles and policies defined in section 10 of Book 2, the payment systems will decide individually whether to adopt the recommendations made in this Bulletin. Payment systems will notify their members of their final decision.

[1] Please refer to EMVCo Notice Bulletin 9 for an explanation of this term (which arises because EMVCo does not project beyond a 10 year horizon). It is recommended that no certificate is issued with an expiry date later than the anticipated lifetime date of the CA key.