

Notice Bulletin No. 25
July 2021

EMVCo Annual RSA Key Lengths Assessment

EMVCo has completed its annual review of the Certification Authority Public Key lengths and expiry dates and makes the following recommendations to EMV-based 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. No certificate should be issued that expires later than the expiry date of the CA key.
- 1984-bit keys are recommended to have an anticipated lifetime to at least 31 December 2031. EMVCo does not project beyond a 10-year horizon. It is recommended that no certificate be issued that expires later than the anticipated lifetime date of the CA key.

Payment systems will decide individually whether to adopt the recommendations made in this Bulletin and will notify their members of their final decision.