

Clarification of Maximum Public Key Lengths

This Specification Bulletin modifies Book 2 in order to clarify the maximum lengths for the Issuer, ICC and PIN Encipherment public keys.

Applicability

This Specification Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 2 Security and Key Management*

Related Documents

- *None*

Effective Date

- *Immediately*
-

Description

This bulletin provides changes to descriptions of the maximum Issuer, ICC and ICC PIN Encipherment Public key lengths in EMV 4.3 Book 2.

This bulletin also draws attention to the additional restrictions on the lengths of moduli as described in Section D1.

Specification Change Notice

EMV 4.3 Book 2 Section 6.1: Keys and Certificates for Offline Dynamic Data Authentication

Please modify the text in Book 2 section 6.1 as highlighted below:

The public key pair of the issuer has a Public Key Modulus of N_I bytes, where $N_I \leq N_{CA} \leq 248$. **N_I may be restricted to less than N_{CA} , see section D1.1 for further details.** If $N_I > (N_{CA} - 36)$, the Issuer Public Key Modulus is divided into two parts, one part consisting of the $N_{CA} - 36$ most significant bytes of the modulus (the Leftmost Digits of the Issuer Public Key) and a second part consisting of the remaining $N_I - (N_{CA} - 36)$ least significant bytes of the modulus (the Issuer Public Key Remainder). **Section D1.1 details additional restrictions on the length of the Issuer Public Key.** The Issuer Public Key Exponent shall be equal to 3 or $2^{16} + 1$.

The public key pair of the ICC has an ICC Public Key Modulus of N_{IC} bytes, where $N_{IC} \leq N_I \leq N_{CA} \leq 248$. ~~N_{IC} may be restricted to less than N_I , see section D1.2 for further details.~~ If $N_{IC} > (N_I - 42)$, the ICC Public Key Modulus is divided into two parts, one part consisting of the $N_I - 42$ most significant bytes of the modulus (the Leftmost Digits of the ICC Public Key) and a second part consisting of the remaining $N_{IC} - (N_I - 42)$ least significant bytes of the modulus (the ICC Public Key Remainder). ~~Section D1.2 details additional restrictions on the length of the ICC Public Key.~~ The ICC Public Key Exponent shall be equal to 3 or $2^{16} + 1$.

EMV 4.3 Book 2 Section B2.1: RSA Algorithm

Please change Book 2 section B2.1 Table 28 and its introduction as follows:

The algorithm produces a cryptogram or digital signature whose length equals the size of the modulus used. The ~~mandatory~~ upper bounds for the size of the modulus are specified in Table 28.

Description	Max. Length
Certification Authority Public Key Modulus	248 bytes
Issuer Public Key Modulus	2478 bytes
Issuer Public Key Modulus (SDA only)	248 bytes
ICC Public Key Modulus	2478 bytes
ICC PIN Encipherment Public Key Modulus	2478 bytes

Table 1: ~~Mandatory~~ Upper Bounds for Size ~~in Bytes~~ of Moduli

Please replace the first paragraph below Table 28 with the following:

The maximum length for issuer and ICC keys is reduced because a 2-byte tag is used for the ICC certificates and ICC keys cannot be longer than issuer keys. For SDA cards the maximum length for issuer keys is 248 bytes because a 1-byte tag is used for the Signed Static Application Data.

Additional restrictions on the lengths of moduli are described in section D1.

Please modify the second paragraph below Table 28 as follows:

In the choice of the lengths of the public key moduli, one should take into account the lifetime of the keys compared to the expected progress in factoring during that lifetime. The ranges (upper and lower bounds) for the key lengths mandated by each of the payment systems are specified in their corresponding proprietary specifications. Further guidance is also provided in the EMV Issuer and Application Security Guidelines.

EMV 4.3 Book 2 Annex D1: Issuer and ICC Public Key Length Considerations

Please replace Annex D1 with the following:

This specification follows the usual convention that allows the Issuer Public Key length to be equal to or less than the CA Public Key length and allows the ICC Public Key and ICC PIN Encipherment Public Key lengths to be equal to or less than the Issuer Public Key length. However, some further restrictions occur due to limitations of the command data structure.

Book 3 section 7 states that records are limited to 254 bytes including tag and length and as a consequence, if an ICC public key pair is required, the Issuer and ICC key lengths need to be less than the CA maximum of 248 bytes.

Book 1 section 9.4.1 states that the maximum number of data bytes that may be sent with a command is 255 and the maximum number of data bytes for a response is 256. If dynamically signed data is included in a response from the ICC, then the latter restriction limits the maximum length of the ICC keys (see section D1.2).

Legal Notice

The EMV® Specifications are provided “AS IS” without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of the EMV® Specifications may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of the EMV® Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement these Specifications is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party’s infringement of any intellectual property rights in connection with the EMV® Specifications