M/Chip Payment System Public Keys

4th December 2018

To ensure proper Mastercard acceptance, acquirers must maintain the correct set of M/Chip Payment System public keys[1] in their terminals that accept contactless transactions or that support offline authentication or offline PIN encryption for contact cards. This applies to all Mastercard products including Mastercard, Maestro and US Maestro.

Thus Acquirers must ensure that their operational terminals

- contain the two 'Live' M/Chip Payment System public keys for RID A000000004[2], namely the keys with index 05 and 06 as specified below.
- do not contain keys other than the operational set of 'Live' keys for RID A000000004. For example, terminals containing test keys may expose the merchant to fraud through the use of fraudulent chip cards exploiting test key presence.

Payment System public keys are typically installed into terminals according to procedures defined by the terminal vendor, for example via a terminal management menu option. Terminals without the Payment System public keys may encounter payment acceptance issues.

The following page provides the values of the two M/Chip Payment System public keys for RID A000000004 along with a 20-byte SHA-1 hash calculated on the concatenation of RID, Index, Modulus and Exponent.

Key Index 05 is a 1408-bit (176-byte) key with an expiry date of 31st December 2024.

Key Index 06 is a 1984-bit (248-byte) key with an anticipated lifetime to at least 31st December 2028. This date represents the current expiry date for this key and the expiration date of issuer public key certificates created using this key is currently limited to being no later than 31st December 2028.

[1] Also known as Certification Authority public keys

[2] This is the Registered Identifier for the Mastercard M/Chip payment application.

RID	A000000004
Index	05
Modulus	B8 04 8A BC 30 C9 0D 97 63 36 54 3E 3F D7 09 1C 8F E4 80 0D F8 20 ED 55 E7 E9 48 13 ED 00 55 5B 57 3F EC A3 D8 4A F6 13 1A 65 1D 66 CF F4 28 4F B1 3B 63 5E DD 0E E4 01 76 D8 BF 04 B7 FD 1C 7B AC F9 AC 73 27 DF AA 8A A7 2D 10 DB 3B 8E 70 B2 DD D8 11 CB 41 96 52 5E A3 86 AC C3 3C 0D 9D 45 75 91 64 69 C4 E4 F5 3E 8E 1C 91 2C C6 18 CB 22 DD E7 C3 56 8E 90 02 2E 6B BA 77 02 02 E4 52 2A 2D D6 23 D1 80 E2 15 BD 1D 15 07 FE 3D C9 0C A3 10 D2 7B 3E FC CD 8F 83 DE 30 52 CA D1 E4 89 38 C6 8D 09 5A AC 91 B5 F3 7E 28 BB 49 EC 7E D5 97
Exponent	03
SHA-1 hash	EBFA0D5D06D8CE702DA3EAE890701D45E274C845

RID	A000000004
Index	06
Modulus	CB 26 FC 83 0B 43 78 5B 2B CE 37 C8 1E D3 34 62 2F 96 22 F4 C8 9A AE 64 10 46 B2 35 34 33 88 3F 30 7F B7 C9 74 16 2D A7 2F 7A 4E C7 5D 9D 65 73 36 86 5B 8D 30 23 D3 D6 45 66 76 25 C9 A0 7A 6B 7A 13 7C F0 C6 41 98 AE 38 FC 23 80 06 FB 26 03 F4 1F 4F 3B B9 DA 13 47 27 0F 2F 5D 8C 60 6E 42 09 58 C5 F7 D5 0A 71 DE 30 14 2F 70 DE 46 88 89 B5 E3 A0 86 95 B9 38 A5 0F C9 80 39 3A 9C BC E4 4A D2 D6 4F 63 0B B3 3A D3 F5 F5 FD 49 5D 31 F3 78 18 C1 D9 40 71 34 2E 07 F1 BE C2 19 4F 60 35 BA 5D ED 39 36 50 0E B8 2D FD A6 E8 AF B6 55 B1 EF 3D 0D 7E BF 86 B6 6D D9 F2 9F 6B 1D 32 4F E8 B2 6C E3 8A B2 01 3D D1 3F 61 1E 7A 59 4D 67 5C 44 32 35 0E A2 44 CC 34 F3 87 3C BA 06 59 29 87 A1 D7 E8 52 AD C2 2E F5 A2 EE 28 13 20 31 E4 8F 74 03 7E 3B 34 AB 74 7F
Exponent	03
SHA-1 hash	F910A1504D5FFB793D94F3B500765E1ABCAD72D9