Visa Smart Debit/Credit Certificate Authority Public Keys

Overview

The EMV standard requires the use of public key technology for Offline Data Authentication, and Offline Enciphered PIN. Each payment system is responsible for maintaining the public root key pairs of its own public key hierarchy in support of the EMV public key infrastructure. Visa distributes the public root keys ("Visa Smart Debit/Credit (VSDC) Certificate Authority (CA) Public Keys" or VSDC CA Public Keys) to acquirers who load them into their terminals. The terminals can thereby check digital signatures from issuers and ICCs at the time of transaction. VSDC acquirers must ensure that the correct VSDC CA Public Keys are loaded into their EMV terminals.

This document contains both production and test keys.

***Important**: Acquirers must ensure that:*

- *Only active and verified production VSDC CA Public Keys are used in their production terminals.*
- *Test VSDC CA Public Keys are not loaded in production terminals.*
- *The 1536-bit key is loaded only into transit fare-gate terminals.*

1 VSDC Certificate Authority Key Summary

Table 1: VSDC CA Production Keys - Status

Key	Expiration Date	Status
1984 bit	31 December 2035 Reviewed annually	Active. Required to be loaded in all VSDC terminals (POS and transit fare gates) supporting Offline Data Authentication or Offline Enciphered PIN.
1536 bit	31 December 2035 Reviewed annually	Active. Intended for use only in transit fare gates supporting Offline Data Authentication. This key must not be loaded into any other type of terminal.
1408 bit	31 December 2024	Expired. This key must not be loaded in production VSDC terminals
1152 bit	31 December 2017	Expired. This key must not be loaded in production VSDC terminals
1024 bit	31 December 2009	Expired. This key must not be loaded in production VSDC terminals

The expiration dates for the currently active VSDC CA keys are reviewed annually. Revised expiration dates are published in a Visa Business News article.

2 VSDC CA Production Public Key Values

This section contains the values for the currently active VSDC CA Production Public Keys.

The Hash value is the SHA-1 hash of RID || Index || Modulus || Exponent.

2.1 1984 Bit Production Key

Table 2: VSDC CA 1984 bit Production Key Value

Component	Value
RID	A0 00 00 00 03
Index	09
Modulus	9D 91 22 48 DE 0A 4E 39 C1 A7 DD E3 F6 D2 58 89 92 C1 A4 09 5A FB D1 82 4D 1B A7 48 47 F2 BC 49 26 D2 EF D9 04 B4 B5 49 54 CD 18 9A 54 C5 D1 17 96 54 F8 F9 B0 D2 AB 5F 03 57 EB 64 2F ED A9 5D 39 12 C6 57 69 45 FA B8 97 E7 06 2C AA 44 A4 AA 06 B8 FE 6E 3D BA 18 AF 6A E3 73 8E 30 42 9E E9 BE 03 42 7C 9D 64 F6 95 FA 8C AB 4B FE 37 68 53 EA 34 AD 1D 76 BF CA D1 59 08 C0 77 FF E6 DC 55 21 EC EF 5D 27 8A 96 E2 6F 57 35 9F FA ED A1 94 34 B9 37 F1 AD 99 9D C5 C4 1E B1 19 35 B4 4C 18 10 0E 85 7F 43 1A 4A 5A 6B B6 51 14 F1 74 C2 D7 B5 9F DF 23 7D 6B B1 DD 09 16 E6 44 D7 09 DE D5 64 81 47 7C 75 D9 5C DD 68 25 46 15 F7 74 0E C0 7F 33 0A C5 D6 7B CD 75 BF 23 D2 8A 14 08 26 C0 26 DB DE 97 1A 37 CD 3E F9 B8 DF 64 4A C3 85 01 05 01 EF C6 50 9D 7A 41
Exponent	03
Hash	1F F8 0A 40 17 3F 52 D7 D2 7E 0F 26 A1 46 A1 C8 CC B2 90 46

2.2 1536 Bit Production Key

***Important**: This key **must only** be loaded in transit fare-gate terminals.*

Table 3: VSDC CA 1536 bit Production Key Value

Component	Value
RID	A0 00 00 00 03
Index	10
Modulus	E9 E7 7C D1 BA B4 88 5B 66 09 D7 92 DF 96 C6 00 65 3D DF 0A 72 89 83 F7 B4 E4 6C BA 53 32 BC 02 6B A4 FB 1C 1A 6D C5 62 EA AD CF 2A 8A E9 87 78 8B 36 80 F1 76 A2 1E E0 87 32 7D B7 45 DD 90 2E 4A 27 33 9B BF 22 A6 78 B5 3C CE E2 3B 36 DC A2 38 DB 8E A3 A6 C3 08 2C C4 D1 14 4C DE 27 93 A2 29 2E 92 3D 0C 94 10 68 C5 C6 7A 8C E7 2D 94 AA 96 D0 CF DB 18 1E 99 60 9E 0C D0 73 14 66 CF 2D 20 B6 5A DB AB 67 6A 69 97 A3 EF 10 A5 B6 C8 87 0D E2 1A E9 78 03 B6 F7 1B 9F 1F 25 DF 53 D6 2B 05 51 76 CF 32 B2 AC C3 64 4F 23 50 F7 38 16 F3 D1 4C 1F B6 D8 D3 06 95 E3 6F 37 7A B0 F4 45 6D
Exponent	03
Hash	BA BB 22 F0 92 C2 69 23 5F FB FD 52 33 85 3A FD 76 9C B6 FA

3 VSDC CA Test Public Key Values

This section contains the values for the currently active VSDC CA Test Public Keys.

The Hash value is the SHA-1 hash of RID || Index || Modulus || Exponent.

***Important**: These VSDC CA Test Public Keys **must not** be loaded in production terminals.*

3.1 1984 Bit Test Key

*Table 4: VSDC CA 1984 bit **TEST** Key Value*

Component	Value
RID	A0 00 00 00 03
Index	94
Modulus	AC D2 B1 23 02 EE 64 4F 3F 83 5A BD 1F C7 A6 F6 2C CE 48 FF EC 62 2A A8 EF 06 2B EF 6F B8 BA 8B C6 8B BF 6A B5 87 0E ED 57 9B C3 97 3E 12 13 03 D3 48 41 A7 96 D6 DC BC 41 DB F9 E5 2C 46 09 79 5C 0C CF 7E E8 6F A1 D5 CB 04 10 71 ED 2C 51 D2 20 2F 63 F1 15 6C 58 A9 2D 38 BC 60 BD F4 24 E1 77 6E 2B C9 64 80 78 A0 3B 36 FB 55 43 75 FC 53 D5 7C 73 F5 16 0E A5 9F 3A FC 53 98 EC 7B 67 75 8D 65 C9 BF F7 82 8B 6B 82 D4 BE 12 4A 41 6A B7 30 19 14 31 1E A4 62 C1 9F 77 1F 31 B3 B5 73 36 00 0D FF 73 2D 3B 83 DE 07 05 2D 73 03 54 D2 97 BE C7 28 71 DC CF 0E 19 3F 17 1A BA 27 EE 46 4C 6A 97 69 09 43 D5 9B DA BB 2A 27 EB 71 CE EB DA FA 11 76 04 64 78 FD 62 FE C4 52 D5 CA 39 32 96 53 0A A3 F4 19 27 AD FE 43 4A 2D F2 AE 30 54 F8 84 06 57 A2 6E 0F C6 17
Exponent	03
Hash	C4 A3 C4 3C CF 87 32 7D 13 6B 80 41 60 E4 7D 43 B6 0E 6E 0F

3.2 1536 Bit Test Key

This key must only be loaded in transit fare-gate terminals.

*Table 5: VSDC CA 1536 bit **TEST** Key Value*

Component	Value
RID	A0 00 00 00 03
Index	89
Modulus	E5 E1 95 70 5C E6 1A 06 72 B8 36 7E 7A 51 71 39 27 A0 42 89 EA 30 83 28 FA D2 80 71 EC EA E8 89 B3 C4 F2 9A C3 BD E4 67 72 B0 0D 42 FD 05 F2 72 28 82 0F 26 93 99 0F 81 B0 F6 92 8E 24 0D 95 7E C4 48 43 54 CD 5E 5C A9 09 2B 44 47 41 A0 39 4D 34 76 65 12 32 47 4A 9B 87 A9 61 DA 8D D9 6D 90 F0 36 E9 B3 C5 2F B0 97 66 BD A4 D6 BC 3B DA DB C8 91 22 B7 40 68 F8 FA 04 02 6C 5F A8 EF 39 8B C3 AB 39 92 A8 7F 6A 78 5C C7 79 BA 99 F1 70 95 66 23 D6 7A 18 EB 83 24 26 3D 62 6B E8 5B FF 77 B8 B9 81 C0 A3 F7 84 9C 4F 3D 8E 20 54 29 55 D1 91 28 19 85 47 B4 7A E3 4D F6 7F 28 BE 43 3F 33
Exponent	03
Hash	71 70 85 0b 97 f8 39 52 04 5c f9 ca 8b 76 12 df eb 69 e9 ef