CHIP AND NEW TECHNOLOGIES

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 terminal population.

This document also includes information regarding the VSDC CA Public Keys used for testing. Acquirers must ensure that:

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

1. VSDC CA Production Public Keys

Table 1–1: VSDC Certificate Authority Public Keys

Effective **immediately**, Visa has adopted the following Visa Smart Debit/Credit (VSDC) Certificate Authority Public Key lengths and corresponding expiration dates.

Key	Expiration Date	Status
1024-bit	**31 December 2009**	This key must have been removed from all devices by **1 July 2013.**
1152-bit	**31 December 2017**	This key must have been removed from all devices by **1 July 2018.**
1408-bit	**31 December 2024**	The 1408-bit CA Public Key is required to be in all VSDC devices supporting Offline Data Authentication or Offline Enciphered PIN. The maximum expiration date for Issuer Public Key certificates will be **31 December 2024**.
1536-bit	Considered to have an anticipated lifetime to at least **31 December 2033**	The 1536-bit CA Public Key is designed for use only in transit fare gates supporting Offline Data Authentication. This key is NOT to be loaded into VSDC POS devices. The maximum expiration date for Issuer Public Key certificates will be **31 December 2033**.
1984-bit	Considered to have an anticipated lifetime to at least **31 December 2033**	The 1984-bit VSDC CA Public Key is required to be in all VSDC devices supporting Offline Data Authentication or Offline Enciphered PIN. The maximum expiration date for Issuer Public Key certificates will be **31 December 2033**.

Table 1–2: 1408-Bit VSDC CA Production Public Key

The 1408-bit VSDC CA Production Public Key is scheduled to expire on **31 December 2024**.

The maximum expiration date for certificates issued with the 1408-bit key will be **31 December 2024**.

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	08
Modulus	D9 FD 6E D7 5D 51 D0 E3 06 64 BD 15 70 23 EA A1 FF A8 71 E4 DA 65 67 2B 86 3D 25 5E 81 E1 37 A5 1D E4 F7 2B CC 9E 44 AC E1 21 27 F8 7E 26 3D 3A F9 DD 9C F3 5C A4 A7 B0 1E 90 70 00 BA 85 D2 49 54 C2 FC A3 07 48 25 DD D4 C0 C8 F1 86 CB 02 0F 68 3E 02 F2 DE AD 39 69 13 3F 06 F7 84 51 66 AC EB 57 CA 0F C2 60 34 45 46 98 11 D2 93 BF EF BA FA B5 76 31 B3 DD 91 E7 96 BF 85 0A 25 01 2F 1A E3 8F 05 AA 5C 4D 6D 03 B1 DC 2E 56 86 12 78 59 38 BB C9 B3 CD 3A 91 0C 1D A5 5A 5A 92 18 AC E0 F7 A2 12 87 75 26 82 F1 58 32 A6 78 D6 E1 ED 0B
Exponent	03
Secure Hash Algorithm –1 Hash	20 D2 13 12 69 55 DE 20 5A DC 2F D2 82 2B D2 2D E2 1C F9 A8

Table 1–3: 1536-Bit VSDC CA Production Public Key

The 1536-bit VSDC CA Production Public Key is currently considered to have an anticipated lifetime to at least **31 December 2033**.

The maximum expiration date for certificates issued with the 1536-bit key will be **31 December 2033**.

The actual key value is available via your local Visa transit contacts.

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	10
Modulus	Contact your local Visa transit contacts
Exponent	03
Secure Hash Algorithm – 1 Hash	Contact your local Visa transit contacts

Table 1–4: 1984-Bit VSDC CA Production Public Key

The 1984-bit VSDC CA Public Key is currently considered to have an anticipated lifetime to at least **31 December 2033**.

The maximum expiration date for certificates issued with the 1984-bit key will be **31 December 2033**.

Component	Value
Registered Application Provider Identifier (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

Secure Hash Algorithm – 1 Hash	1F F8 0A 40 17 3F 52 D7 D2 7E 0F 26 A1 46 A1 C8 CC B2 90 46

2. VSDC CA Public Test Keys

Table 2-1: 1408-Bit VSDC CA Public Test Key

This is the VSDC CA Public 1408-bit **TEST** key.

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	92
Modulus	99 6A F5 6F 56 91 87 D0 92 93 C1 48 10 45 0E D8 EE 33 57 39 7B 18 A2 45 8E FA A9 2D A3 B6 DF 65 14 EC 06 01 95 31 8F D4 3B E9 B8 F0 CC 66 9E 3F 84 40 57 CB DD F8 BD A1 91 BB 64 47 3B C8 DC 9A 73 0D B8 F6 B4 ED E3 92 41 86 FF D9 B8 C7 73 57 89 C2 3A 36 BA 0B 8A F6 53 72 EB 57 EA 5D 89 E7 D1 4E 9C 7B 6B 55 74 60 F1 08 85 DA 16 AC 92 3F 15 AF 37 58 F0 F0 3E BD 3C 5C 2C 94 9C BA 30 6D B4 4E 6A 2C 07 6C 5F 67 E2 81 D7 EF 56 78 5D C4 D7 59 45 E4 91 F0 19 18 80 0A 9E 2D C6 6F 60 08 05 66 CE 0D AF 8D 17 EA D4 6A D8 E3 0A 24 7C 9F
Exponent	03
Secure Hash Algorithm -1 Hash	42 9C 95 4A 38 59 CE F9 12 95 F6 63 C9 63 E5 82 ED 6E B2 53

Table 2–2: 1536-Bit VSDC CA Public Test Key

This is the VSDC CA Public 1536-bit **TEST** key.

The actual key value is available via your local Visa transit contacts.

Component	Value
Registered Application Provider Identifier (RID)	A0 00 00 00 03
Index	89
Modulus	Contact your local Visa transit contacts
Exponent	03
Secure Hash Algorithm – 1 Hash	Contact your local Visa transit contacts

Table 2–3: 1984-Bit VSDC CA Public Test Key

This key is the VSDC CA Public 1984-bit **TEST** key, exponent 3.

Component	Value
Registered Application Provider Identifier (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
Secure Hash Algorithm –1 Hash	C4 A3 C4 3C CF 87 32 7D 13 6B 80 41 60 E4 7D 43 B6 0E 6E 0F