Visa Business News

Chip Cards

26 September 2019

Visa Smart Debit / Credit Certificate Authority Annual Key Assessment

Global | *Acquirers, Issuers, Processors*

Visa Network

Overview: The Visa Smart Debit / Credit Certificate Authority (CA) has extended the expiration date of the 1984-bit CA key. The expiration date of the 1408-bit CA key has not changed.

Each Visa Smart Debit / Credit (VSDC) or Visa contactless card that supports Offline Data Authentication (ODA) or Offline Enciphered PIN must contain an Issuer Public Key (IPK) Certificate that is provided to the issuer by the VSDC Certificate Authority (CA) and signed by a VSDC CA Private Key. To validate the certificate and recover the data it contains, which is necessary to successfully complete ODA or Offline Enciphered PIN, the terminal must contain the corresponding VSDC CA Public Key.

VSDC CA keys are scheduled to expire while they are still considered secure. Visa has assessed the expiration dates based on EMVCo recommendations and Visa security reviews. As a result of the assessment, **effective immediately**, the expiration dates are as follows:

- **31 December 2024** for the Production VSDC CA 1408-bit Public Key (expiration date unchanged)
- **31 December 2029** for the Production VSDC CA 1984-bit Public Key (expiration date extended by one year; previous expiration date was 31 December 2028)

Issuer Impact

Issuers may continue to use expiration dates of up to 31 December 2024 on their cards with certificates signed by the VSDC CA 1408-bit key.

Issuers may now request certificates signed by the VSDC CA 1984-bit key with an expiration date of up to 31 December 2029.

Note: To ensure that IPKs are considered secure, certificates that expire after 31 December 2019 must be for IPKs that are at least 1408 bits long.

Acquirer Impact

Acquirers must ensure that all terminals that support ODA or Offline Enciphered PIN contain the 1408-bit and 1984-bit production VSDC CA keys with correct expiration dates (if expiry dates are coded into the terminals). These are also identified by the Public Key Index (PKI). The PKI 08—1408-bit key and the PKI 09—1984-bit key are the only keys that should be used in devices. All other Visa Public Keys must be removed.

Key Points

The VSDC CA provides three key lengths to issuers: a 1408-bit certificate, a 1536-bit certificate (for Host Cloud Emulation in support of Transit Only) and a 1984-bit certificate.

Visa issuers may personalize certificates signed by the 1408-bit or the 1984-bit CA key on their cards as long as the expiration date of the card does not exceed the expiration date of the certificate.

The VSDC CA will reject:

- Any request to the 1408-bit CA where the IPK is longer than 1408 bits or if the certificate expiration requested is after 31 December 2024.
- Any request to the 1536-bit CA where the IPK is longer than 1536 bits or if the certificate expiration requested is after 31 December 2029.
- Any request to the 1984-bit CA where the IPK is longer than 1976 bits or if the certificate expiration requested is after 31 December 2029.

The VSDC CA will not sign certificates for IPKs shorter than 1152 bits and IPKs shorter than 1408 bits that expire after 31 December 2019, as summarized in the table below:

Issuer Key Size	VSDC CA Key Size	Latest Certificate Expiration Date
1152-bit	1408-bit	31 December 2019
1408-bit	1408-bit	31 December 2024
1408-bit	1984-bit	31 December 2029
1976-bit	1984-bit	31 December 2029

Acquirers must ensure that the correct Visa public keys (i.e., 1408-bit and 1984-bit) with correct expiration dates are loaded into the terminals supporting ODA or Offline Enciphered PIN.

Note: This information applies to all Visa regions (including Europe) and certificates on both six- and eight-digit Bank Identification Numbers (BINs).

For More Information

Merchants and third party agents should contact their acquirer.