NEW

6.2.1. Manage Public Keys

Description	Obtain an Issuer Certificate from the Visa Certificate Authority (CA) and load that value onto chip cards as part of the personalization process.
EST. Duration	The Visa Certificate Authority will deliver Issuer Certificates within one week of the request date, assuming no errors in paperwork and encryption processing.
Dependencies	▪ Authenticity of issuing institution and the authority of its representative has been validated by the region, using criteria outlined by the Visa Certificate Authority. ▪ Paperwork request has been completed. ▪ An agreement has been made about a secure transmission method between issuer and Visa CA.

Chip Card Payment Service uses RSA (Rivest, Shamir, and Adleman) public key technology in the Static Data Authentication process. Static Data Authentication is a cryptographic process between the card and the terminal that validates the static data on the card and protects issuers against counterfeiting. As part of this process, the Issuer Certificate, an encrypted public key value that resides on the card, is validated by the terminal to verify that the card was issued by a valid issuer. Refer to the following figure for details on how the Issuer Certificate and public keys are used during Static Data Authentication.

The Visa Certificate Authority is the Visa International body that manages the generation and distribution of public key information used for chip transaction processing. The region acts as the liaison between the issuer and the Visa Certificate Authority to complete enrollment with the Visa Certificate Authority and to provide the issuer with an Issuer Certificate.