iCVV - Protection of the magnetic stripe in the migration to chip

A Risk Management and Security White Paper

1. Summary

The Visa Smart Debit and Credit (VSDC) specification requires all chip cards to contain the full magnetic stripe data (Track 2), including the Cardholder Verification Value (CVV) on the chip.

The magnetic stripe data on the chip is in the same format as the data on the magnetic stripe on the card. Therefore if may be possible to use the data to create a counterfeit magnetic stripe card for subsequent fraudulent use in non-chip enabled terminals.

To limit this exposure, the VSDC payment application allows the Issuer to use a different CVV, named the iCVV (integrated circuit card Card Verification Value), when the same account information is stored on a chip card. This allows Issuers to identify fraudulent transactions from counterfeit magnetic stripe cards that have been produced using the magnetic stripe data compromised from a chip card.

The use of iCVV on chip cards therefore represents a simple but highly effective solution to mitigate risk during the transition from magnetic stripe to chip technology.

The iCVV technique can also be used to protect a magnetic stripe image when it is stored on non-card devices such as mobile phones when they are used for payments. One such example is proximity payments which occurs when a mobile phone is used to transmit beam the magnetic stripe details to the POS terminal using infrared transmission.

Visa regulations stipulate that effective 1 January 2005 all **new** Visa Chip Card Issuers must certify support for iCVV in the magnetic stripe data encoded on the chip.

This paper provides guidelines to Issuers and their designated processors to help them implement the iCVV.

2. Fraud exposure

In the magnetic stripe world today, several countries are now starting to experience a new type of account compromise called wire-tapping. This involves the capture of magnetic stripe data as it is transmitted from the POS terminal to the Acquirer's host through either public or private networks. This information is then copied to either a counterfeit, lost or stolen card, and used to perform fraudulent transactions.

During the migration to chip when there will be both chip and magnetic stripe cards and terminals in the market, the magnetic stripe technology is still very vulnerable. The magnetic stripe data stored on the chip card may be compromised, even when a chip card is accepted in a chip card terminal, because this data is read from the chip and transmitted in authorization messages in each chip transaction.

Possible compromise scenarios include the following:

- By reading the data directly from the chip itself.
- By capturing the data within the chip card terminal during transaction processing, using a terminal 'implant' in a similar way as it is done by criminals today in the magnetic stripe world.
- By capturing the data sent from a chip card terminal either using wire-tapping, as described above, or wherever data may be stored during transmission or processing, for example in Third Party Processors' or Acquirers' hosts.

3. Implementing iCVV in New Payment Solutions

The magnetic stripe data is also used in some new payment solutions. For example, in proximity payments the magnetic stripe data is stored in the mobile phone, either in a SIM chip card or in the device memory. This data is subsequently transmitted to the POS terminal for transaction processing. The iCVV can also be used in these environments to prevent fraud. This is of particular importance if the data is transmitted over non-encrypted wireless connections.

4. The iCVV Solution

iCVV is today an optional risk control feature that enables Issuers to detect when magnetic stripe data contained on chip cards, or other payment devices, is being fraudulently used in magnetic stripe transactions. Issuers include a unique iCVV value in the magnetic stripe data on the chip thereby distinguishing it from the CVV encoded on the physical magnetic stripe of the card.

The iCVV uses the:

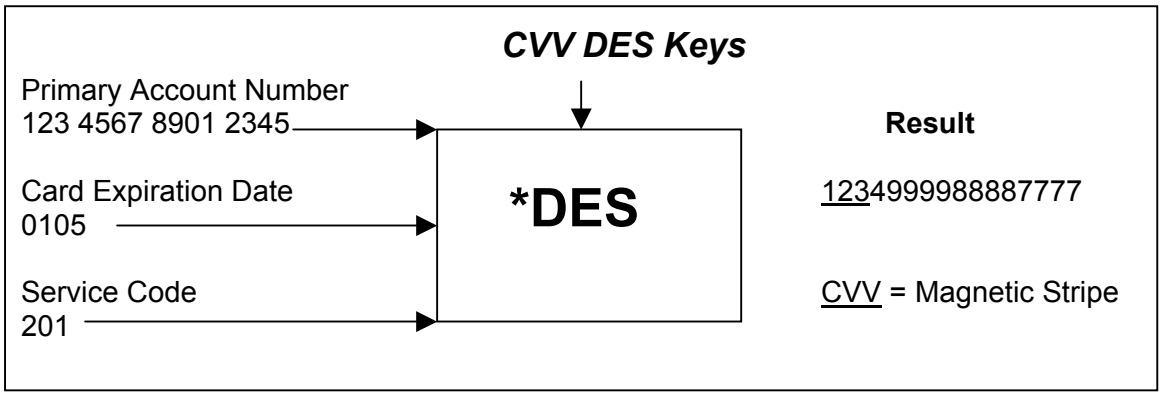
- Same CVV algorithm as for CVV calculation;
- Same network and Host Security Modules messages;
- Same CVV DES key(s) and management.

The only change is that the issuer manipulates one of the pieces of data used to create the CVV value prior to calculation or validation. The Service Code used in calculating the CVV value for the magnetic stripe CVV is replaced, (only for the calculation of the iCVV), with a value of 999 to create the new iCVV for the magnetic stripe image in the chip. This manipulation is required in the iCVV creation *and* validation.

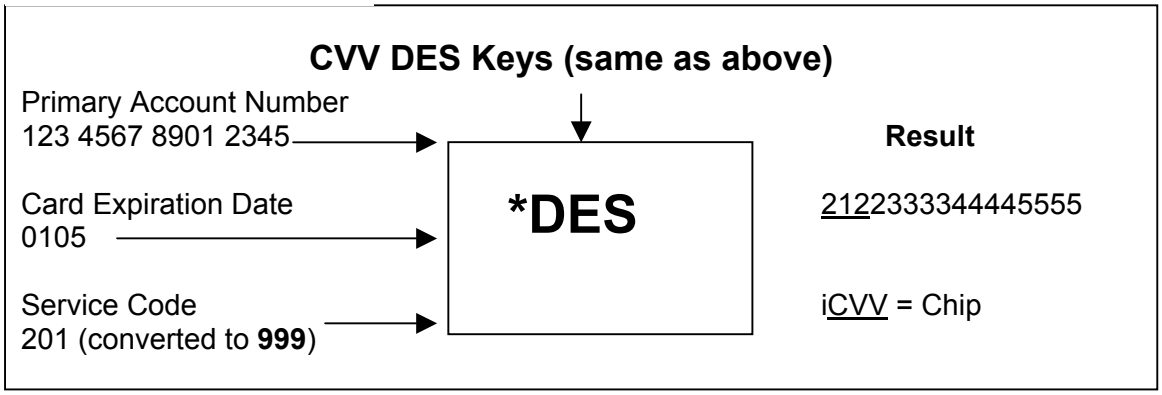
5. How it works

The diagrams below illustrate how the iCVV is calculated. It also illustrates how the standard CVV is calculated for comparison.

Magnetic Stripe CVV



Chip iCVV



see 10.

6. Impact on issuers

Issuers electing to perform their own CVV validation will need to modify host systems to perform iCVV or CVV checking depending on whether the transaction is chip or magnetic stripe read (indicated by the POS Entry Mode Code of 05 or 90).

7. Impact on Acquirers

There are no changes required by merchants or acquirers to be able to accept and successfully transmit the iCVV data. However, acquirers must ensure that authorization messages contain the correct POS Entry Mode Code (05-chip or 90-magnetic stripe read) as issuer systems rely upon this value to determine whether the iCVV or CVV should be checked to verify the card. If the wrong information is given to the issuer, they might decline a valid transaction.

8. Impact on Visa Stand-In Processing (STIP)

Issuers also utilize VisaNet 'CVV stand in processing' service, which allows VisaNet to perform CVV checking on their behalf. The same service will be used for iCVV checking. VisaNet will perform the appropriate iCVV or CVV checking depending on the value of the POS Entry Mode Code (05 or 90) and pass on the result of the check to issuers, i.e. passed or failed iCVV checking.

The issuer's authorization and routing decisions made for CVV processing will also apply to iCVV, so there is no need to change or adjust to be able to process iCVV. VisaNet also uses the same stand-in parameters or iCVV as the issuer selected for CVV.

For issuers participating in Visa Card Authentication Service, VisaNet will forward both results of iCVV/CVV checking and Card Authentication checking to the issuer irrespective whether they have pass or failed verification. In case of only iCVV or CVV failure, if STIP is invoked for generation response, a response code 05 is sent to the Acquirer (i.e. decline).

9. New Asia Pacific iCVV Operating Regulation

The Operating Regulation detailed below was approved at the Visa International Asia Pacific Board meeting in October 2003. This approval serves to encourage issuers to implement the iCVV to protect themselves and the overall confidence of the chip card payment solution. Refer to Asia Pacific Member letter APML43/03 for details.

- Effective 1 January 2005 all new Visa Chip Card Issuers must certify support for iCVV in the magnetic stripe data encoded on the chip.

10. Reference

- Please refer to the document *Payment Technology Standards Manual*, 1 September 2002, for more information and implementation of iCVV.