

ACCEPTING SAFE TRANSACTIONS THE SMART WAY



MAKE THINGS HAPPEN



NEDBANK

INDEX



2	SMART CARDS AND EMV CHIP TECHNOLOGY
4	BENEFITS TO MERCHANTS
6	IMPACT ON MERCHANTS
8	RECOGNISING SMART CARDS
10	MAGSTRIPE vs SMART CARDS
12	SMART-CARD FUNCTIONS
22	MERCHANT READINESS CHECKLIST
24	FREQUENTLY ASKED QUESTIONS

SMART CARDS AND EMV CHIP TECHNOLOGY



Internationally, chip technology is being introduced to migrate card payments from magstripe cards to smart cards. The South African banking industry is following this trend. Merchants play an important role in accepting foreign and local smart cards.

Smart cards, also known as chip cards, represent a new generation of cards with a silicon computer microchip embedded in the plastic. Smart cards can store more data and support processing functions that are not possible with magstripe cards. In addition, smart cards can hold software for multiple payments and rewards programmes, offering merchants and customers a new level of utility and convenience.

For merchants, the benefits of smart cards include reducing the risk of fraud and chargebacks. Encrypted information on the chip validates the smart card as being genuine in each transaction. Customers are required to enter a PIN and do not have to sign at the point of transaction.

The EMV (Europay, MasterCard and Visa) Forum in South Africa was established to introduce smart-card standards in South Africa. The forum comprises the four major banks, Nedbank, ABSA, Standard Bank and First National Bank, as well as other financial institutions, working together to implement chip technology in the card payment systems.



BENEFITS TO MERCHANTS

Cost savings, increased efficiencies
and new opportunities



1 Use of a PIN vs a signature

- Using a PIN will reduce the number of disputed transactions between merchants and customers.
- Merchants are no longer responsible for verifying the customer as the true cardholder by checking the signature. Chip technology will authenticate the cardholder regardless of whether the authorisation was sought online or approved offline (eg the transaction was below the floor limit).
- There will be fewer circumstances in which chargebacks will be allowed against merchants.

2 Reduced fraud and improved security

Online transactions:

- The smart card will be verified by the issuing bank to confirm that the card is genuine.

Offline transactions:

- Unlike magstripe cards, which can be 'skimmed', information on a smart card is virtually impossible to copy. Smart cards use a new encryption technology that authenticates the card as being genuine at the point of sale.

3 Efficiencies and opportunities

- Smart cards mean cost reduction, as there are lower telecommunications traffic and central processing time.
- Customers' smart cards can also be programmed with merchant rewards and other value-add programmes.

IMPACT ON MERCHANTS





It is important for merchants to ensure that POS devices are chip-enabled, ie POS devices have the requisite hardware and software to accept smart cards and process data from the chip.

Previously, merchants carried most of the risk and liability for fraudulent transactions. But now the liability for fraudulent transactions has shifted to the party who isn't compliant with EMV chip technology. So, if a fraudulent transaction could have been prevented by chip technology, but the card issuing bank or the owner of the POS device (merchant/bank) wasn't compliant, then the bank or retailer will be liable. Who is the liable party will be determined following an investigation.



RECOGNISING SMART CARDS





There are many different types of card design and style. However, there are some common features on all smart cards:

- A chip with either gold/silver foil in the top left-hand side of the card is present.
- The following details should always be present:
 - Expiry date
 - Cardholder name



- Magstripe (in future, all cards will have a holographic magstripe)
- Signature panel – note the reduced length
- Name of the issuer



MAGSTRIPE vs SMART CARDS



Current magstripe transactions

- 1 Swipe card to read the magstripe.
- 2 Type in the last four digits of the card number.
- 3 Type in the total amount due.
- 4 Print voucher and receipt.
- 5 Request customer's signature.
- 6 Verify signature with the signature on the back of the card.
- 7 Provide receipt and return card.



Smart-card transactions

- 1 Insert smart card into chip reader. Do not remove for the duration of the transaction.
- 2 Select application if applicable, eg CREDIT, CHEQUE or SAVINGS.
- 3 Select the type of transaction, eg SALE, REFUND or CASH BACK.
- 4 Type in the total amount due.
- 5 Request customer to type in his or her PIN.
- 6 Wait for the PIN to be verified.
- 7 NedLink device will authorise the transaction and issue a customer and merchant receipt. Remove and return the card and receipt to customer.

Notable differences:

- The customer typing in his or her PIN will become the primary method of verifying cardholders. It will no longer be the signature.
- Magstripe cards are swiped but smart cards are inserted into the chip reader and must remain there for the duration of the transaction. **Early removal of a smart card will result in the cancellation of the transaction.**

SMART-CARD FUNCTIONS





The following operations guide applies to all NedLink smart devices that have been enabled for EMV chip technology.

Loading EMV profile

The EMV profile will be automatically loaded onto the NedLink device. It's important to ensure that the profile was successfully loaded. If unsuccessful, no sales transactions can be processed.

Three sets of messages will be printed on the POS slip to indicate whether the profile was successfully loaded and at what time. For example, if the EMV profile was loaded at 12:00, the following messages will be printed on the receipt:

12.00	LOADING PROFILE
12.01	SUCCESSFUL
12.01	LOADING EMV PROFILE
12.01	SUCCESSFUL
12.01	LOADING EMV KEYS
12.01	SUCCESSFUL

Manual loading of EMV profile

If there is a power failure or other such event, the EMV profile and keys must be manually loaded following these steps:

- Insert merchant card into the back of the NedLink device.
- Press F1.
- Press 2 for UTILITIES.
- Press 2 for DOWNLOAD.
- Press 1 for PROFILE.



Key prompts

The following are some of the important messages displayed on the NedLink smart device.

PROMPT	WHAT DOES THE PROMPT MEAN?	NEXT STEP
USE CHIP READER	The card has a chip present; the smart card should not be swiped like a magstripe card.	Insert the smart card into the chip reader.
PROCESSING ERROR	The smart card has been removed from the chip reader before the transaction has been processed.	Reinsert the smart card and reinitiate the transaction.
CANCEL	The smart card has been removed from the chip reader before the transaction was completed or the cancel button was pressed.	Reinsert the smart card and reinitiate the transaction.
SELECTION • CREDIT • CHEQUE • SAVINGS	This means that the customer has more than one application linked to his or her smart card.	Request the customer to choose the relevant application.
SELECTION • SALE • CASHBACK • PRE-AUTH • REFUND • BALANCE ENQUIRY	Select the type of transaction based on whether it's a sale or refund, etc. A balance enquiry is not permissible on credit card applications.	Make the selection and wait for the transaction to be processed.
ENTER AMOUNT R0.00	Type in the total amount due.	Type in the total amount due from the customer.
AMNT: RXX.00 F2: YES F3: NO	Request for confirmation of the total amount entered.	Check for any errors in the entering of the digits and select F2 to confirm or F3 to decline.
ENTER CLIENT PIN	The customer is required to enter his or her four-digit PIN. Some banks may require a five-digit PIN to be entered.	Request the customer to enter his or her PIN and then ENTER.
PIN OK	The PIN is being authenticated.	Wait for authentication to be completed.
WAITING FOR AUTH REPLY	The transaction is being processed.	Wait for the processing to be completed.



Cardholder verification methods (CVM)

PIN

The NedLink smart device will prompt for a PIN only when the issuing bank requires a PIN on the card. Where a PIN is required, no signature line will be printed on the receipt. Customers should not be asked to sign for the transaction where there is no signature line on the receipt.

Signature

All smart cards will carry a magstripe and a signature panel on the back of the card. The signature panel will be reduced in length. The signature still remains the international default for cardholder verification and is the default for many local card transactions.

The procedures for checking smart-card transactions verified by means of a signature remain the same as they are today.

Transactions with no CVM

A transaction may be processed without cardholder verification in the following instances:

- in environments where POS terminals are unattended (eg ticket vending machines) or at tollroad operations.
- where the smart card has been personalised by the issuing bank so that no PIN or signature is required (eg to allow for fast processing of offline authorised transactions).

Note: Even where the smart card is programmed for no CVM, it's possible for the NedLink smart device to request another form of CVM (either PIN or signature).

Budget transactions (credit cards)

Local credit cardholders may have a budget option available where the transaction value is R300 or more. Follow these steps to facilitate a customer purchasing on budget:

- Insert smart card into the chip reader.
- Select application on the PIN pad. Use the F-key on the PIN pad to scroll between the different applications and then press the green button to select the CREDIT application. Budget transactions may only be performed on credit cards.
- Press 1 for SALE (or the number that corresponds to SALE) from the menu.
- ENTER AMOUNT R0.00 prompt displayed. Type in the total amount due.
- AMNT: RXX.00 F2: YES F3: NO prompt displayed. Press F2 to confirm or F3 to correct a mistake on the total amount due.
- BUDGET PERIOD prompt displayed. Type in the number of months required. The customer may choose any period between 3 and 60 months. Type 6 for a six-month budget option.
- ENTER CLIENT PIN prompt displayed. Request your customer to type in his or her PIN on the PIN pad and press ENTER.
- PIN OK prompt displayed. Please wait for PIN verification.
- WAITING FOR AUTH REPLY prompt displayed. Please wait for the processing to be completed.
- NedLink device will authorise the transaction and issue a customer and merchant receipt. Remove and return the card and receipt to customer.





Refund transactions (credit cards)

- Insert smart card into the chip reader.
- Prompt displayed on PIN pad to select application, eg CREDIT, CHEQUE or SAVINGS, if applicable.
- Request your customer to choose the relevant application.
- Use the F-key on the PIN pad to scroll between the different applications and then press the green button to select the application.
- Press 4 for REFUND (or the number that corresponds to REFUND) from the menu.
- MERCHANT PASSWORD prompt displayed on the PIN pad. A supervisor must type in the merchant password or swipe his or her supervisor card.
- ENTER AMOUNT R0.00 prompt displayed. Type in the refund amount. Press F2 to confirm or F3 to correct a mistake on the total amount due.
- REFUND SUCCESSFUL prompt will be displayed.

Note: It is not necessary for customers to enter their PIN for a refund transaction.

Reversal transactions (debit cards)

To process a reversal on a smart card please follow these steps:

- Insert smart card into chip reader.
- The following menu will be displayed*: CHEQUE, SAVINGS.
- Request your customer to choose the relevant application.
- Use the F-key on the PIN pad to switch between the different applications and then press the green button to select the application.
- Press 5 for REVERSAL (or the number that corresponds to REVERSAL) from the menu.
- MERCHANT PASSWORD prompt displayed. A supervisor must type in the merchant password or swipe his or her supervisor card.
- TRACE NUMBER prompt displayed. Type in the trace number found on the original transaction slip.
- ENTER CLIENT PIN prompt displayed. Request your customer to type in his or her PIN and press ENTER.
- PIN OK prompt displayed. Please wait for PIN verification.
- WAITING FOR AUTH REPLY prompt displayed. Please wait for the processing to be completed.
- REVERSAL SUCCESSFUL prompt will be displayed.
- NedLink device will authorise the transaction and issue a customer and merchant receipt. Remove and return the card and receipt to customer.

* If the smart card is a single-application card, the terminal will skip directly to the transaction menu.



Authorisations

Offline vs online authorisation

Some transactions will be processed offline, while others will be processed online. These differences should not be viewed as an error and the transaction and/or customer should not be treated differently. Offline transactions might be processed faster than online transactions.

When a transaction is approved offline, a PIN may still be required. Offline transactions do not mean that no CVM is required. The NedLink smart device has the capability to verify offline the PIN encoded on the customer's smart card.

There are three types of authorisations for NedLink devices:

- **Offline authorisation** occurs when the transaction amount is below the floor limit and within the risk parameter limits set on the smart card. The transaction is approved without verification from the bank.
- **Online authorisation** occurs when the transaction is above the floor limit or outside the predefined risk parameters set on the smart card. The transaction is authorised by the bank. The introduction of smart cards will reduce the number of online authorisations. NedLink devices may randomly select transactions to go online regardless of the parameters on the card.



- **Telephone authorisation** occurs where the merchant calls the bank to obtain approval. With the introduction of smart cards, telephone authorisation will only be required if the transaction was supposed to go online and could not be approved offline. In the event where a telephone authorisation is provided, the merchant must enter a manual authorisation override code to conclude the transaction.

Telephone authorisation

PLEASE CALL prompt will be displayed where telephone authorisation is required. Keep the following numbers handy:

Visa/MasterCard authorisation
0860 321 222

American Express® authorisation
0860 321 555

Diners Club authorisation
011 358 8500

To proceed with a manual authorisation override, a merchant password is required. When a supervisor card is issued, a PIN is also provided.

Your NedLink smart device will prompt for an authorisation code, 'ENTER AUTH NO'. Follow the prompt and key in the approval code from your telephone authorisation.



Manual transactions

Current procedures remain unchanged for manual transactions.

Manual transactions allow a card to be processed without swiping or inserting it into the chip reader. This function should be used with extreme caution and is only permissible if so stipulated in your contract and agreed to by Nedbank Limited. If approved, the manual transaction profile will be loaded onto the merchant profile. Remember, always take an imprint of the cardholder's card. Please note that your NedLink smart device requires a nine-digit authorisation code.

If telephone authorisation is obtained, follow these steps:

- Press F4.
- Select the type of card:
 - Press 1 for credit, buy-aid or RCS cards
or
 - Press 2 for garage or fleet cards.
- ENTER CARD NUMBER prompt displayed. Type in the card number.
- EXP DATE (MMYY) prompt displayed. Type in expiry date in required format.
- Type in the CVV2/CVC2 number (last three digits on the back of the card) and press ENTER.
- 1 SALE/2 REFUND prompt displayed. Press 1 for SALE.
- ENTER AMOUNT R0.00 prompt displayed. Type in the total amount due.
- MERCHANT PASSWORD prompt displayed. A supervisor must type in the merchant password or swipe his or her supervisor card.
- PRE-AUTH YES or NO prompt displayed. Press F2 for YES if an authorisation code has been telephonically obtained.
- Type in the authorisation number.

If no authorisation was obtained, press F3 when the ENTER AUTH NO prompt is displayed. The transaction will go online for authorisation.



Fallback transactions

The magstripe may only be used where the chip is damaged or the NedLink device is malfunctioning. Magstripe transactions done on smart cards are known as 'fallback' transactions. All fallback transactions go online for authorisation, hence zero floor limit applies. Apply normal magstripe card acceptance rules for fallback transactions.

Note: For fallback transactions a merchant password or supervisor card and PIN may be required.

Key prompts

PROMPT DISPLAYED	WHAT DOES THE PROMPT MEAN?	NEXT STEPS
USE MAGSTRIPE	This message means that the NedLink device is unable to read the chip on the smart card. In this situation, the NedLink device will 'fallback' to magstripe transaction. Magstripe transactions will be processed online.	<ol style="list-style-type: none"> 1 Swipe the card like an ordinary magstripe card. 2 Type in the total amount due by the customer. 3 Request the customer to enter his or her PIN (if the device prompts for PIN entry) or sign for the transaction (if the device prompts for signature). Whether a PIN or signature is requested depends on the bank issuing the card.
ENTER CLIENT PIN	The customer has entered his or her PIN incorrectly.	The customer has the option to reenter his or her PIN.
WAITING FOR AUTH REPLY	<p>The customer has entered his or her PIN incorrectly three times.</p> <p>The customer does not have the option of reentering his or her PIN and has been blocked from using the card application.</p>	The transaction will go online to require the bank that issued the card to approve/decline the transaction. If declined, request the customer to pay using an alternative method, eg cash.

Declined transactions

A declined smart-card transaction cannot be reinitiated using the magstripe. Current operating procedures should then be followed for declines and failures, such as asking the customer to use an alternative method of payment.

Typing in credit card numbers

Visa International does not permit manually keying in the customer's card number to process smart-card transactions.

MERCHANT READINESS CHECKLIST



Training staff and supervisors

TRAINING REQUIREMENTS	YES/NO	ACTION REQUIRED
1 Do your cashiers know how to accept smart cards?		
2 Do your supervisors know how to handle exceptional events, such as fallback transactions?		
3 Have the following topics been covered in your training?		
• What does a smart card look like? How is it different to a magstripe card?		
• How does the transaction process differ between magstripe cards and smart cards?		
• What can cashiers do to help customers who have forgotten their PIN or been blocked from use of their card?		
• Under what circumstances should a cashier refer to or request help from a supervisor?		

Helping cashiers and serving customers

It is important to take into consideration that cashiers and customers will require easy access to the NedLink device at the point of sale. Customers may have disabilities, such as poor sight, dexterity or poor memory, which could impact on their use of PIN pads. Some customers may also require assistance with the operation of the PIN pad and keeping their PIN secure.

The following tips may help merchants prepare for the introduction of smart cards.

Accessibility

- Ensure that the NedLink device can be easily reached by cashiers and customers.

Physical setting

- Station the NedLink device on a counter or table.
- Test whether a customer in a wheelchair can access the NedLink device.

Security

- Place the PIN pad so that the security cameras do not point directly to the PIN pad.
- Place the PIN pad in such a position so as to ensure that others standing behind cannot see the customer entering his or her PIN.
- Place the PIN pad in such a position so as to ensure that cashiers cannot see the PIN being entered.
- Ensure that the NedLink device is secured so that it cannot be stolen or damaged.
- Store the NedLink device out of sight when it's not in use.

Operational

- Test that the NedLink device does produce duplicate receipts, one for the customer and another for the merchant.

FREQUENTLY ASKED QUESTIONS



1 Why introduce smart cards?

Smart cards are being introduced to reduce fraud. Did you know that:

- one in every thousand credit card transactions is fraudulent?
- in 2005 card fraud cost South Africa over R100 million and the trend is for this figure to increase each year?
- credit card fraud is used to fund organised crime in South Africa?

Customers' smart cards have the capability of supporting add-on services, such as merchant reward programmes and multiple payment applications.

2 How does the chip work to secure a card?

The chip uses encryption technology to authenticate the card and ensure that it is genuine. Before the card is issued, data unique to the card is encrypted in the chip and is known only to the card issuing bank. At the time of a transaction the terminal will request this encrypted information from the card (offline). Once the card has been validated as genuine, the transaction can proceed.

3 Can smart cards be used in existing electronic terminals?

Yes, by swiping the magstripe to process a transaction. The chip can be read and processed only by terminals that are chip-enabled.

4 When will I see smart-card volumes increase at my NedLink devices?

Currently, international smart cards and local pilot production smart cards are in circulation and rollout will increase from the second quarter of 2006. Local banks will phase in the issue of smart cards on renewal or replacement of magstripe cards.

5 What happens if the customer enters the wrong PIN?

If the customer enters the incorrect PIN once or twice, he or she will be prompted to try again.

If the customer enters his or her PIN incorrectly three times consecutively, even if at separate locations, his or her card application will be blocked. In this situation direct your customer to contact his or her bank.

6 What happens if the customer has forgotten his or her PIN?

Customers who have forgotten their PIN have to contact their bank directly.

7 What should I tell the customer who has forgotten his or her PIN or who has been blocked from using a card application?

Request the customer to pay using another payment method.

8 Where can customers get more information?

Customers should receive information from their bank when they receive their smart cards. For more information customers must contact their bank directly.



MERCHANT HELPDESK NUMBER

0860 114 966

www.nedlink.co.za

Nedbank Ltd Reg No 1951/000009/06

We subscribe to the Code of Banking Practice of The Banking Association South Africa and, for unresolved disputes, support resolution through the Ombudsman for Banking Services. We are an authorised financial services provider.