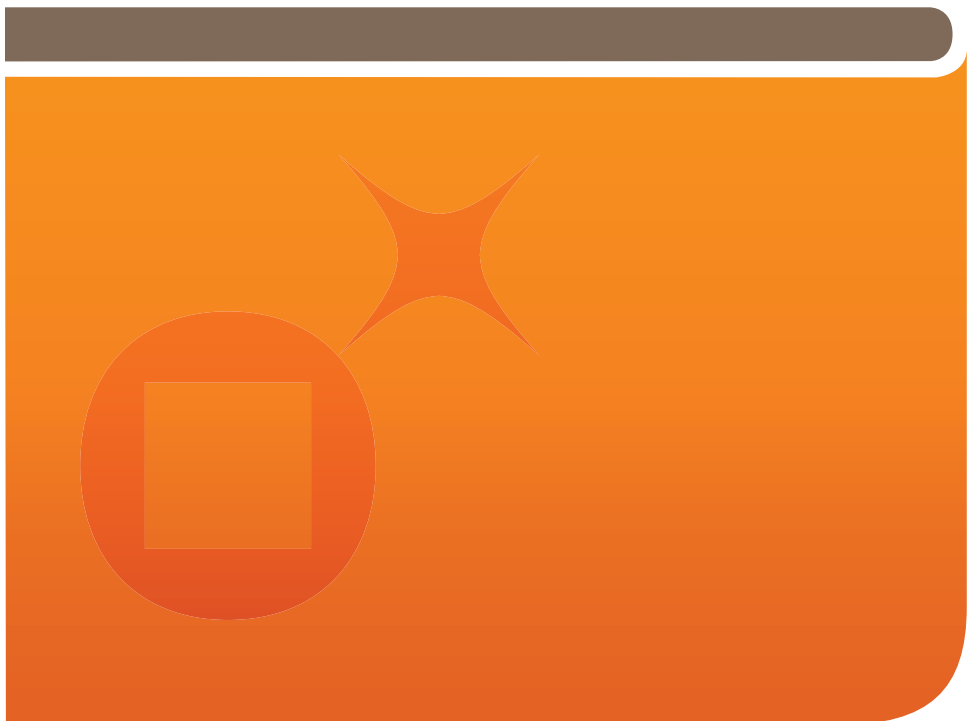




Gemalto Explains

# Smart Bankcards

How EMV\* smart bankcards protect you from fraud



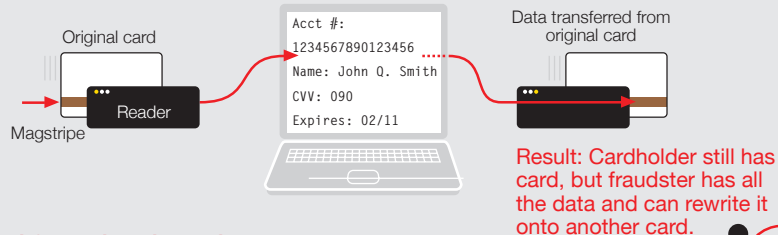
## How it works

# Smart bankcards\*\*

### Magstripe cards are open to fraud

#### ...from skimming

Swiping a card through an (illegal) magstripe reader (skimming) makes it possible to produce a clone of the card, with all its relevant data intact.



#### ...and from data breaches

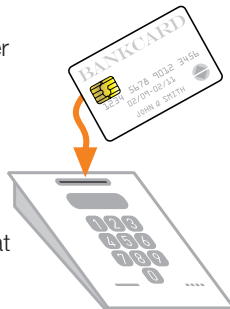
When account numbers are stolen from card databases, unauthorized shopping is possible because the physical card is not needed.



### Smart bankcards prevent fraud at retail point-of-sale

- 1 At the store or other retail outlet, the card is placed into a device that reads the data on it.

Contactless cards can also be used (at different terminals).



- 2 Enter individual PIN code.



- 3 The card checks the PIN stored on the card.
- 4 Prepares the transaction before sending it to the bank.
- 5 Keeps track of offline transactions.
- 6 The issuer sets transaction rules (for instance, floor limits, cumulative amounts, velocity, when last online, etc.).

The computer inside the smartcard is an active part of the transaction, unlike the magstripe, which is passive.

### Dynamic data authentication

The transaction flow of EMV smart bankcards at point-of-sale

#### DDA confirms:

- The card is authentic, because only a card issued by a bank could contain a valid signature.
- The card is present.
- The cardholder is present, because a PIN has been entered.

#### Using a private key, the chip on the card calculates:

- Unique **digital signature** for each transaction, by using inputs from the terminal to make an algorithm.
- This **algorithm** contains a number of elements, including the transaction amount, the time/date, the merchant ID, and a random number...
- ...and this sent from the terminal to the **bank for authorization** via the network.

Using the **public key** to check the digital signature, the terminal can verify that the card is authentic.

### Smart bankcards prevent fraud online

- 1 Place card into reader.
- 2 Enter PIN number.
- 3 Reader generates one-time-password (OTP).
- 4 OTP is typed into computer.
- 5 A USB reader, plugged directly into your computer, can also be used.
- 6 In addition, phone orders can have card-present authentication.

As with point-of-sale transactions,

#### DDA confirms:

- The card is authentic.
- The card is present.
- The cardholder is present.

Result: The same assurance of security at home or work as you do at a terminal in a retail store, because only the card you hold can generate this OTP.

## How it works

# Smart card technology

### What is smart card technology?

Smart card technology uses a computer and software with 100s of built-in security features.

The contacts on the surface of the device are connected...



...to wires running from a computer chip under the surface.



The whole piece is embedded into a plastic card or hard token.

### Smart card benefits:

**No swiping** The smart card chip is used for authorization instead of a magnetic stripe.

**No skimming** Each smart bankcard has a unique identifier and a digital seal that cannot be copied or cloned and put onto another card; the banks will know that it is a fake, and will refuse authorization.

**No online fraud** The card is supplied with a device that generates a different one-time-only password each time the card is used online.

**Strengthens card-present security** The card is an active part of the transaction.

**With a reader**, the user has card-present security for online banking and payments (previously known as card-not-present).

\* EMV is a global standard for smart bankcards managed by EMVCo, and jointly owned by American Express, JCB, MasterCard, and Visa.

\*\* More than 700 million EMV bankcards are used worldwide. (Source: EMVCo)