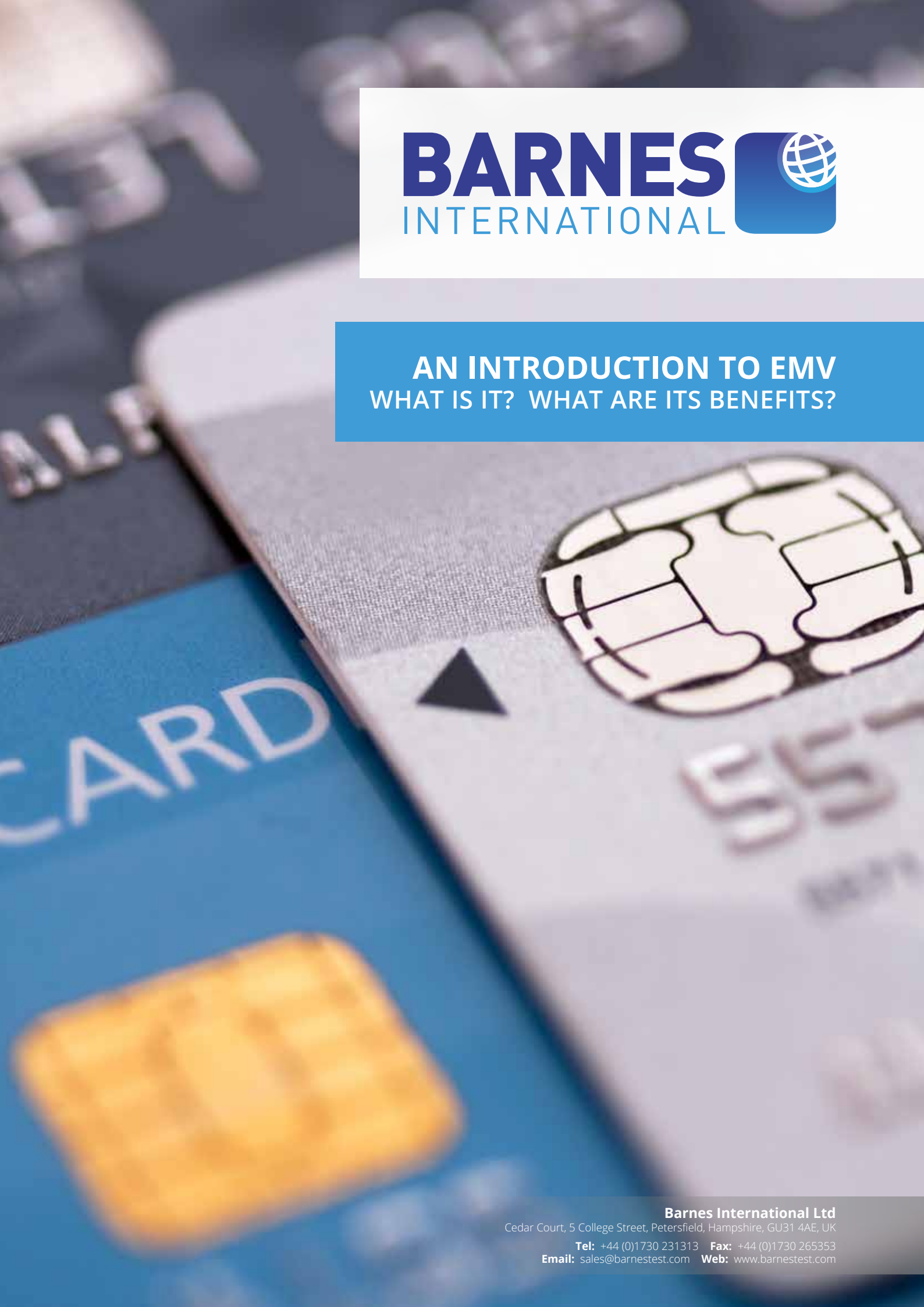

BARNES INTERNATIONAL

AN INTRODUCTION TO EMV

WHAT IS IT? WHAT ARE ITS BENEFITS?

Barnes International Ltd
Cedar Court, 5 College Street, Petersfield, Hampshire, GU31 4AE, UK
Tel: +44 (0)1730 231313 **Fax:** +44 (0)1730 265353
Email: sales@barnestest.com **Web:** www.barnestest.com

WHAT IS EMV?*

EMV represents a set of specifications that enable smart (chip-based) payments cards to be used at POS terminals around the world to provide secure payment transactions.

The specifications are created, maintained and enhanced by EMVCo, an organisation jointly owned and resourced by all the major international payment card schemes – Visa, MasterCard, American Express, JCB, (China) UnionPay and Discover. EMV specifications and other documents are publicly available on the EMVCo website www.emvco.com.

Outside the US, and as of May 2012, 45% of payment cards (1.5 billion cards) and 76% of payments terminals (22 million terminals) were based on EMV technology. The growth rate has been, and continues to be, impressive.

A wide range of certified and field-tested products and services support this worldwide infrastructure. Not only EMV cards and terminals, but also card personalisation, network and issuer and acquirer host systems.

EMV cards are rapidly replacing payment cards based on magnetic stripe and signature technologies. These technologies from the 1960s have been shown to be insecure, being easily copied and modified. This led to high levels of fraud – one of the main drivers behind EMV.

Many national (mainly debit) card payment schemes have also adopted the EMV specifications. In fact prior to EMV, the French banks introduced their own smart debit card – the "Carte Bancaire". Another driver behind EMV was the perceived danger of different countries developing their own (incompatible) smart card schemes. France was one of the first countries to migrate to EMV.

* EMV = Europay, MasterCard & Visa, the original payment scheme members

The EMV specifications concentrate on the interfaces between the card and the terminal, and between the card and the issuer host systems. Digital security is provided by standard cryptography – RSA public key cryptography between the card and the terminal, and triple-DES (symmetric) cryptography between the card and the issuer host system.

Behind the interfaces, the core processes, for example risk management, are specified by the payment schemes. EMV terminals are type-approved by EMVCo-certified test laboratories; EMV cards are approved by the payment schemes which also carry out end-to-end (card-to-host) testing before the cards are issued - to ensure global interoperability.

CONTACTLESS EMV CARDS

Contactless cards were not included in the original EMV specifications, and were introduced by the major payment schemes independently. This had the unfortunate effect of creating different card-terminal message interfaces. The lower level protocol was fixed, based on the ISO 14443 standard. The separate specifications for the terminal software kernels are published by EMVCo and are used in the EMV terminal type approval process.

Contactless EMV cards are used for low value transactions not requiring cardholder verification. Typical usage is at coffee bars, fast-food restaurants, cinemas and small convenience stores. Contactless card reading is typically built in to a customer PIN/ contact reader device. This enables EMV contact transactions to take place for higher value purchases, and purchases when the offline spending limit has been exceeded. Contactless EMV cards have also started to be used for mass transit fares, for example in London.

NFC* MOBILE DEVICES

EMVCo has published guidelines for the use of NFC mobile devices (e.g. smartphones, tablets) for contactless EMV transactions. The NFC specifications include ISO 14443 and so at the protocol level NFC devices are able to communicate with EMV contactless terminals. Messages can also be exchanged, and the NFC device can at a basic level emulate a contactless EMV card.

There have been a large number and variety of NFC payment trials around the world. However widespread implementation has not yet occurred. This is mainly due to a lack of agreement on the technology required in the mobile device, and the lack of an overall business case.

FUTURE DEVELOPMENTS

EMV future developments will include:

- Further work on NFC mobile device acceptance.
- "Tokenisation" of the card account number or PAN for secure remote payment transactions. This will protect against the theft of transaction data.
- A next generation of specifications for cards and terminals that will include greater standardisation and the inclusion of a new public key algorithm (ECC**).

* NFC = Near Field Communications
** ECC = Elliptic Curve Cryptography

WHAT ARE THE BENEFITS OF EMV?

FOR CARD ISSUERS

For card issuers the reduction in the level of card fraud is a major benefit. In particular fraud involving the counterfeiting or cloning of cards, and the misuse of lost or stolen cards.

Counterfeit Card Fraud

EMV cards cannot be counterfeited, or at least have not been counterfeited so far. Even if technically possible, it would not be economically feasible. To be certain, the issuer can decide to use dynamic data authentication (DDA) to authenticate the card. DDA uses a private RSA key in the card, rather than static data authentication (SDA) which authenticates a specified set of card data. The mass production of counterfeit cards that has been used with magnetic stripe cards is no longer possible. Countries that have implemented EMV have seen this type of fraud plummet, apart from non-domestic transactions in countries that have not yet migrated to EMV.

Lost & Stolen Card Fraud

The misuse of lost or stolen cards is best countered by using a PIN. This can either be verified online at an issuer host system, or offline in the EMV chip. Countries that have migrated from magnetic stripe cards to EMV cards without migrating from signature to PIN will still suffer from fraud using lost/stolen cards. With an EMV card this type of fraud can be mitigated by "blocking" the card application when a transaction goes online to the issuer host system.

Fraud on EMV chip-and-PIN cards-not-received (intercepted in the mail) can be prevented or reduced if the use of the PIN is mandatory for all transactions. As with PIN-based magnetic stripe cards, PINs are sent separately to the cardholder.

In EMV countries, fraud migrates to other channels – non-EMV terminals and ATMs (cross-border fraud), internet-based transactions and other "card-not-present" transactions.

In order to limit fraud migration to non-EMV terminals and ATMs, and to encourage the implementation of EMV cards and terminals, payment schemes have used "liability shifts". Liability for preventable fraud is allocated to the card issuer or the transaction acquirer who has not implemented EMV. This has resulted in EMV terminals being installed in tourist locations popular with international tourists, even where the country concerned has not implemented EMV cards.

An additional benefit for issuers is the reduction in the cost of handling disputed transactions. With an EMV transaction the issuer can be confident that the card in question has been used as indicated, and if applicable, that the correct PIN was entered. The onus is then on the cardholder to state how the card and PIN were used without his/her knowledge.

The risk management in the issuer host system benefits from the additional EMV transaction data, and from the ability to modify the data in the card or even block the card application, using issuer script commands sent in the authorisation response message.

FOR RETAILERS

For the retailer there are also benefits. With EMV chip-and-PIN transactions the retailer cashier is no longer responsible for authenticating the card or verifying the signature of the customer. In fact the cashier doesn't need to see or touch the card. The POS terminal doesn't need to print out a second receipt for signature, and the retailer doesn't need to store the signed receipts, and retrieve them for disputed transactions. EMV transactions are faster and easier.

FUTURE OPPORTUNITIES

For both issuers and retailers the ability to support secure offline transactions opens up the opportunity to expand card acceptance to new locations. These may be unattended locations like vending machines, or high throughput locations like mass transit turnstiles. Lower value transactions can become economically attractive.

Many of these new opportunities involve contactless EMV cards, and use the benefits of fast and easy transactions. Future EMV cards will tend to be "dual interface" cards, able to be used for both contact and contactless transactions.

The continued increase in the numbers of EMV cards and terminals, the extension of the EMV specifications, the evolution of supporting technologies and the new acceptance opportunities augur well for the future of EMV.

ABOUT THE AUTHOR

Richard Johnstone is an experienced EMV consultant. He worked for APACS during the first EMV implementation and then for 12 years for MasterCard Worldwide at their Chip Centre of Excellence. As an independent consultant he has worked on a variety of EMV-related assignments. For Barnes International he provides customised EMV training and consultancy, based around a two-day EMV course.

ABOUT BARNES

Barnes International is the world leader in the development and supply of Chip Card Test Tools and Magnetic Stripe Analysers. Barnes world class Test Tools enable the manufacture and issue of valid magnetic stripe, contact and contactless EMV chip cards, ensuring quicker approval by Payment Schemes and minimising pre-issue costs. Its Test Tools for Laboratory, Manufacturing and Bureau include QC testing to ISO, EMV, Amex, JCB, MasterCard, Visa, CUP, Discover, Interac, SPAN, GlobalPlatform and GSM specifications. Barnes also offers EMV Consultancy and Card Testing. For further information on Barnes' products and services go to www.barnestest.com