

Banking Automation **BULLETIN**



Growing demand for multivendor software

Future of ATM software lies in integrated solutions

Multivendor – multiple choice

New business opportunities for chip and PIN

UK online fraud rate 50% higher than that of North America

Country profile: Slovenia



EMV CHIP

New business opportunities with chip and PIN

By Nick Collin, Banking Technology Consultant

EMV technology has not yet been widely applied to CNP transactions, and as a result, levels of CNP fraud are increasing fast

The manner and timing in which infrastructure-based applications develop typically follows a pattern of industry hype then disillusionment before progress is established

There are outstanding opportunities for banks to leverage the new chip and PIN infrastructure with added value applications, according to RBR's latest report *EMV Chip Applications: Catching the Next Wave*. In western European countries where there is a critical mass infrastructure of EMV chip cards and terminals, banks are already beginning to develop new markets and card acceptance outlets with innovative chip-based applications. Banks in regions which are still in the process of migrating from old magnetic stripe technology to chip and PIN, or have not yet started, have opportunities to learn from the experience of the pioneers and build added value features into their emerging EMV infrastructures from the outset.

Success in reducing card fraud

The main objective of chip and PIN migration is reduced card fraud, and this has been successfully achieved in countries such as the UK and France where levels of domestic, face-to-face fraud have indeed dropped dramatically. Levels of 'fraud abroad' involving non-chipped cards or terminals are still high, but this will improve as more and more countries migrate. The report predicts that even the USA, hitherto resistant to EMV technology, will eventually be unable to resist the momentum of global migration.

EMV technology has not yet been widely applied to card-not-present (CNP) transactions via the internet and telephone, and as a result, levels of CNP fraud are increasing fast – now accounting for over 50% of card fraud in the UK, for example. This is about to change. An EMV application which is increasingly well-established in Europe for secure online banking is remote chip authentication (RCA), in which a cardholder enters the PIN into a simple card reader to generate a one-time-password (OTP) which is then used to authenticate the transaction. More than 15 million RCA readers have been deployed across Europe by major banks, including Barclays and RBS

in the UK. The natural next step is to combine RCA with the 3D Secure protocol, increasingly familiar to online shoppers in the form of MasterCard SecureCode and Verified by Visa. By treating the OTP as a 3D Secure password, this enables strong, two-factor authentication of CNP payments, and is expected to be a critical factor as the card payments industry struggles to maintain dominance in the burgeoning e-commerce payments market against non-card alternatives such as PayPal.

Gaining traction for new applications

The manner and timing in which infrastructure-based applications develop is complex and difficult to predict, typically following a pattern of first industry hype then disillusionment before real progress is established. The RBR report explores a number of models to help banks understand likely developments and plan ahead with more confidence.

Contactless payments is an interesting case in point. The same chip which supports EMV payments also supports contactless 'Tap & Go' operation using either a plastic card or an NFC-enabled mobile phone. This development has been enthusiastically embraced by the card payments industry as a key weapon in the 'war on cash'. Contactless smartcards are indeed well established in niche markets, including mass transit systems such as London's Oyster Card, and there are excellent opportunities for banks to deploy branded contactless EMV payment cards in these environments. But although the current industry hype is that such deployment will spread rapidly to a much more general class of low value, high volume outlets, displacing cash, this may be constrained by 'chicken and egg' issues. No matter how many contactless cards are issued, until there is a critical mass infrastructure of readers in place, the volume of new contactless payment transactions will remain tiny.

Conversely, embedded within the contactless payment proposition is another EMV application known as pre-authorised payment – effectively a

new form of e-purse – which may in time come to be seen as an example of premature industry disillusionment. The chip-based e-purse concept has been around for a long time and has had mixed success. Although schemes such as Germany's Geldkarte and Belgium's Proton have gained some traction in their local markets, volumes have remained disappointingly low, and cross-border deployment has been minimal. The reason is that they are based on proprietary e-purse solutions and require special terminals; so there is lack of interoperability between schemes, and a patchy acceptance infrastructure.

The EMV pre-authorised payment solution, in contrast, can be used at any EMV terminal, anywhere in the world. Moreover, since it uses the superior risk-management capabilities of the EMV chip to control spending and reloading of pre-paid funds, it is a very safe payment product which can be issued to anyone and be used securely in predominantly offline acceptance environments such as contactless payments. Despite a few pilot deployments, pre-authorised payment has not yet been a success in its stand-alone, contact form. However, this may be because the regions where it has most potential – the huge unbanked or underbanked markets in the developing world – are precisely those regions where EMV migration has yet to gain momentum. This may be one to watch in the longer term.

Another EMV application with great potential is the multi-payment card. Such cards are loaded with more than one standard payment application – typically debit and credit – and the terminal prompts the user to choose which method of payment to use. This is a very simple, but potentially very powerful example of how banks can leverage EMV chips to improve customer recruitment and retention, card activation and usage. Surprisingly, banks have only recently started issuing multi-payment cards, but the results have been impressive, in countries ranging from Finland to Taiwan. This may be because it was not widely understood that acceptance of multi-payment

cards is a standard feature of all EMV EFTPOS terminals. The manner in which different terminals prompt choice of payment method is still somewhat variable, and this may be a challenge in terms of cardholder and merchant education. Nevertheless, as more experience is gained, the prediction is that this application will enjoy rapid and widespread deployment in the near term.


High potential for use with other technologies

The EMV chip story is further complicated by the development, in parallel, of other technologies. In the early days of chip development, it was expected that the data storage capacity of chip cards would be widely exploited for offline applications. Such applications have indeed been developed; mass transit ticketing and payment applications must almost always be offline, and offline chip-based loyalty applications have enjoyed considerable success, particularly in Turkey. But in recent years there has been a revolution in telecommunications technology with the result that online processing is now almost as fast, reliable and cost-effective as offline processing. In the future we are likely to see increasing deployment of hybrid EMV solutions, with most processing and data storage occurring on remote servers in near-real-time, and the chip card acting mainly as a secure token for accessing the online applications.

This model underpins an exciting new breed of 'entitlement applications'. Many types of payment are associated with some form of cardholder entitlement, such as social benefits and discounts, age-related concessions (or prohibitions), health treatment, government services, membership, or physical access. By securely loading a branded EMV chip card with appropriate entitlement indicators, the cardholder can be identified, entitlements authenticated, and the associated payment recalculated and processed in one single, streamlined transaction. This type of application requires not

The multi-payment card is a very powerful example of how banks can leverage EMV chips to improve customer recruitment and retention, card activation and usage

The EMV chip story is complicated by the development, in parallel, of other technologies



www.sbs.co.at

SBS
Salzburger Banken Software

- More than 20 years of experience in ATM software
- Running 140 different models of ATMs, cash-recycling systems and non-cash terminals in more than 25,000 installations
- Monitor and manage your ATM network with high-quality data
- Make your own ATM solution based on our multivendor ATM development platform

Banks wishing to catch the next wave of EMV applications need to treat chip as a strategic, whole-bank issue

- ▶ just special programming of terminals, but also partnerships between the institutions from different sectors, and for this reason will take time to become widespread, but the potential is huge.

Entitlement schemes exist all over the world. In Russia, for example, 70% of citizens belong to such schemes, administered for the most part using highly labour-intensive, expensive and unreliable paper-based systems. Smartcard solutions are indeed quite widely deployed and known variously as 'community', 'city', or 'campus' cards, but these tend to be local, proprietary solutions and suffer from the usual problems of lack of interoperability and the need for specialised terminals. There is a big opportunity for innovative banks to add value in these

situations by leveraging their EMV infrastructures. An excellent example of how this can work is provided by Santander, which has issued an astonishing 3.7 million campus cards to 185 universities in 11 countries. Today, these cards are multi-application EMV cards supporting a wide range of student ID and other entitlement applications, but also, crucially, standard branded debit card payments.

A key message of the RBR report is that banks wishing to catch the next wave of EMV applications need to treat chip as a strategic, whole-bank issue, understood by senior management and deployed with vision and commitment across all divisions and functions. ■

For more information, please visit: www.rbrlondon.com/emvchip

ONLINE FRAUD

UK online fraud rate 50% higher than that of N America

North America's e-commerce market burgeoned before the UK's, and online merchants have had longer to hone their fraud management practices

January saw the simultaneous release by CyberSource, the provider of electronic payment, risk and security management solutions, of their latest annual reports on online payment fraud in North America (Canada and USA) and the UK. These were based upon surveys of 352 online merchants in North America and over 200 online merchants in the UK.

There was a large disparity in the size of the two e-commerce markets in 2009 – estimated North American online sales were \$275 billion versus UK online sales of £54.8 billion (\$85.7 billion) – but the two CyberSource reports illustrate that there were often similarities in the approaches taken by online merchants to detect and counteract fraud. Despite the use of similar tactics, UK merchants incurred a fraud rate 50% higher than their North American cousins, and were only half as successful in disputing fraud reason-coded chargebacks.

Lowest ever fraud rate in North America

North America's e-commerce market burgeoned before the UK's, and online merchants have had

longer to hone their fraud management practices. As a result, North America had managed to reduce payment fraud to just 1.2% of online revenues in 2009, the lowest-ever proportion, continuing a downward trend from 3.6% in 2000, 1.8% in 2004 and 1.4% in 2008. The absolute value of online merchants' payment fraud losses fell for the first time to an estimated \$3.3 billion in 2009, a \$700 million saving on 2008.

There was also an encouraging fall in the proportion of accepted orders that were later determined to be fraudulent, which decreased to 0.9% in 2009, the lowest ratio ever recorded. Online merchants in the consumer electronics sector reported the highest fraudulent order rate of 1.5% due to the nature and value of the goods.

The UK report estimated that the sampled online merchants' payment fraud losses in 2009 were 1.8% of revenues, one and a half times the loss rate in North America, which would amount to total fraud losses in the UK of £850 million (\$1.3 billion). These estimated losses are over triple the expected annual value of card-not-present fraud in the UK.

Banking Automation **BULLETIN**

Regular topics include:

- ATM hardware and software
- Branch banking
- Biometrics
- Cash usage and handling
- Contactless payments
- Internet banking
- EMV and smart cards
- EFTPOS
- e-purse
- Interchange fees
- ISO/IAD activity
- Merchant acquiring
- Mobile payments/banking
- Outsourcing
- P2P payments
- Payment and loyalty cards
- Payment systems
- Prepaid cards
- Regulatory changes
- Security and fraud
- Self-service equipment
- Teller automation



A unique source of news and analysis of key issues in banking technology, cards and payments

- Independent and authoritative insights from industry experts
- Detailed country profiles including proprietary ATM and cards market data in every issue
- Exclusive extracts from RBR's industry-leading market research reports
- Comprehensive industry conference diary
- Read by senior executives in over 90 countries worldwide

Published since 1979

The Bulletin keeps you on top of your industry agenda – can you afford not to subscribe?

For more information about subscribing or advertising please visit www.rbrlondon.com/bulletin

PRIORITY ORDER FORM Banking Automation Bulletin

Subscription period

Printed

- One year (12 issues) **£650** (€750/\$1040)
 Two years (24 issues) **£1100** (€1265/\$1760)
 Three years (36 issues) **£1500** (€1725/\$2400)

Electronic and printed* Standard (1-5 users)

- £975** (€1120/\$1550)
 £1650 (€1900/\$2640)
 £2250 (€2590/\$3600)

Multi-user (6+ users)

- £1950** (€2240/\$3120)
 £3300 (€3800/\$5300)
 £4500 (€5200/\$7200)

* Including one print subscription

PAYMENT METHOD

Please invoice me or By payment card Visa MasterCard Amex JCB

Card no Expires / Total payable

YOUR DETAILS

Title (Mr, Ms, Dr) _____ First name _____ Surname _____

Position/Department _____ Company _____

Address _____

Tel _____ Email _____

VAT (TVA) no _____ Signature _____ Date _____

The information contained in Banking Automation Bulletin may not be reproduced or copied in any form, or be placed on a company intranet, without prior written permission from Retail Banking Research Ltd.

Please return to **RETAIL BANKING RESEARCH** 304 Sandycombe Road, Kew Gardens, Richmond, Surrey TW9 3NG, UK
 Tel: +44 (20) 8940 1398 Fax: +44 (20) 8940 1527 Email: bulletin@rbrlondon.com Web: www.rbrlondon.com/bulletin