SMART PAYMENT ASSOCIATION

shaping the future of payment technology

PIN distribution by SMS

A SPA's White paper

November 2012

Table of Contents

1. Executive summary

In stark contrast to today's ultra-connected online lifestyles, the primary method for distributing credit and debit card PIN codes to cardholders remains the postal service. It is slow, outdated, with inherent security weaknesses.

There is, however, an opportunity to change all this.

As detailed in this paper, PIN by SMS distribution offers the opportunity for card issuers to get PINs into the hands of their consumers faster, more cost effectively and more securely than ever before.

Today's consumers will not wait. They can access their bank accounts online, download apps wherever and whenever they are, and manage their lives on the move. Having to wait 2 to 3 days for a PIN to come through the mail is something of an anachronism in the digital world.

PIN by SMS offers a wholly customer-centric solution to this problem – increasing loyalty and enabling an instant response to customer requests.

From a balance sheet perspective, getting the PIN to the cardholder with the minimum of delay increases the speed of card activations, and eliminates revenue leakage of unused and dormant cards. Models within the paper suggest issuers are able to gain additional revenues of up to and above 750,000 USD annually by utilising PIN by SMS.

Security is also enhanced. SMS adds a crucial secondary distribution channel to the card issuance process – eliminating the risk of paper PIN mailer interception.

And then there's the high cost of conventional distribution – from the environmental wastage of paper-based PIN mailers, through to the financial burden of postal charges.

The technology is available and opportunities are immense. It is time to take PIN distribution into the digital age. This paper delivers all the information you need to make the smart choice.

2. Introduction

The purpose of this SPA whitepaper is to offer a detailed analysis of the emerging PIN by SMS distribution process. A 'must read' document for all financial institutions considering adoption - from payment card issuers, prepayment card bodies and other connected service providers - the paper investigates the opportunities of this new, more convenient and money saving delivery mechanism.

2.1. Context

The world is a very different place from that of the middle of the 1970s when a plastic card first became widely adopted as an instrument for performing a financial transaction.

Advancements in information technology, increased living standards and the huge investments in modern communication infrastructures have changed the way consumers pay for goods and services, and how financial institutions manage those transactions.

Today, the Personal Identification Number (PIN) has never been so important to both cardholders and issuers. When the PIN first began life over five decades ago its primary purpose was one of an identification mechanism – part of the authorisation process for cash withdrawals at Automatic Teller Machines (ATM). In more recent times the PIN has moved on. It is now adopted as a method of authenticating a cardholder in an EMV Point-Of-Sale (POS) transaction, replacing the cardholder signature. This change has been driven by the need for increased security and to combat fraud for physical transactions where a card is present.

Yet while the PIN's role has evolved, the way in which it is issued to cardholders has not. Now, as in the mid 1970s, the most common method of issuing a PIN is via a paper-based PIN mailer, distributed using postal services. While there have been developments in the physical attributes of the PIN mailer itself, this method remains characterised by slow delivery, ever increasing postal costs, and weaknesses in security.

2.2. Scope

Due to the role played by SPA Members in PIN management the focus of this paper is on the issuance of a PIN to a cardholder. This includes the initial issuance of PIN, and the reminder or re-issuance of a forgotten PIN.

While other forms of non-paper PIN issuance exists, this paper focuses solely on the use of SMS as a means for the cardholder to securely retrieve their PIN.

The paper considers how issuers can harness existing technology in order to deliver PIN by SMS to the cardholders in the manner most appropriate to our digital age.

2.3. Definitions

PIN
In the context of this white paper the PIN is the 4 to 6 digit Personal Identification Number used to authenticate a cardholder during ATM or POS* transactions using a given payment card. This is the number entered by the cardholder onto a PIN pad at either an ATM or POS terminal. The PIN plays an important role in securing a transaction, and as such it is imperative that PIN data is a secret only shared between the cardholder and the issuer.

** The PIN has absolutely no connection to codes used to unlock mobile phones or similar devices.*

PIN Generation
The PIN is generated in a specific data generation system hosted by the bank (or service provider). The PIN generation system provides data to the PIN distribution system. These processes must be separated.

PIN Distribution
A personalisation service provider is involved in the personalisation of PIN data onto the card at issuance. They may also be involved in the production of the PIN mailers distributed to the cardholder to inform them of an initial generated PIN, or a reminder of a lost or forgotten PIN.

PIN Usage
The typical usage of a PIN can vary depending on the type of card. For example, a credit card is typically not to be used at an ATM for cash withdraws. As a result, unless a PIN is required for a POS transaction, a credit card cardholder may not know or remember the initial PIN.

Offline PIN / Online PIN
An offline PIN is used in EMV offline transactions (with risk management being handled offline by card and POS). An online PIN is not stored on the payment card. It can be used for EMV or magnetic stripe cards, and is systematically checked online by the bank's back end systems.

2.4. Growing PIN and mobile phone usage

Traditional payment cards have evolved in many parts of the world and now rely on the EMV global standard using smart cards and PIN verification. However, this evolution has yet to occur in some developed countries – most notably the United States. That country's card payment industry still relies on magnetic stripe technology. Nevertheless, the general trend is towards EMV & PIN, and smart card migrations are developing apace in many regions of the world – typically triggered by the need to reduce payment card fraud (see chapter 7.2.).

According to EMVCo (refer to chart 1 below), 45% of all payment cards in global circulation are based on EMV technology. According to these figures, EMV smart cards represent at least 1.5 billion payment cards in circulation worldwide. As smartcard market share increases, magnetic stripe card shipments will continue to decline – despite magnetic stripe card volumes currently exceed those of EMV smart payment cards.

According to SPA, its member organisations shipped 898 million smart cards in 2011 – 90% of which were EMV smart cards. This reflects a 12% year-on-year growth rate.

Potentially, PIN by SMS distribution has an addressable market that far exceeds this, at more than 3 billion units.

Chart 1: Worldwide EMV Deployment and Adoption in Q4 2011

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribbean	318,779,062	41.1%	4,443,000	76.7%
Asia Pacific	366,229,237	28.2%	4,551,000	51.4%
Africa & the Middle East	31,573,578	20.6%	462,000	75.9%
Europe Zone 1	759,760,119	84.4%	11,920,000	94.4%
Europe Zone 2	37,104,467	14.5%	610,500	68.1%
United States†				
TOTALS	1,513,446,463	44.7%	21,986,500	76.4%

* Figures reported in Q4 2011 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally.

† Figures do not include data from the United States.

Visa Inc. and MasterCard announced plans to accelerate EMV migration in the United States by 2015. Similarly, in a move that will further accelerate the drive towards ubiquitous adoption of EMV & PIN, American Express and Discover have issued road maps for EMV adoption.

In parallel with developments within the smart card sector, global mobile phone subscriptions grew from less than 1 billion in 2000 to over 6 billion today, according to figures released by the World Bank. The vast majority of the market is located in developing countries (over 80%). However, in the developed world mobile phone penetration has reached (and in some case exceeded) 100%. The developed countries are also leading the charge from feature phones to smartphones, with penetration of these fairly new devices already approaching 50%

With the ubiquity of the mobile phone is it becoming increasingly difficult to resist the premise that the handset is fast becoming the most effective device through which to reach customers in a timely and efficient manner, anytime and anywhere.

Adding another interesting dimension to the debate, international tourist arrivals have grown for seven of the last ten years, according to the World Tourism Organization (UNWTO). Tourist sending has also been on the rise despite the recent economic slowdown – with the largest spending levels being reported within EMV countries where EMV & PIN is already deployed or mandated within the next few years. Europe, the United States and China are all good examples. Therefore, it is highly likely that international travellers will soon expect their issuing banks to have the capacity to deliver lost or forgotten PIN numbers to them, wherever they are in the world.

The growth of EMV, the mobile explosion and the growing mobility of the world's population all underline the growing importance of alternative methods of PIN delivery. Against this background paper-based solutions no longer seem fit for purpose. PIN by SMS, on the other hand, appears logical. Usage is expected to increase rapidly in line with demand.

3. Benefits

3.1. Generates additional revenues

3.1.1. Initial PIN with new payment card

The traditional paper-based delivery of a PIN creates a delay between the issuance of the PIN and the usability of the card - as it must be printed and sent by postal mail.

By contrast the immediacy of the PIN by SMS distribution model massively reduces the delay for both issuer and cardholder – typically eliminating the 2 to 3 business day wait experienced under the conventional paper process.

PIN by SMS places the PIN in the hands of the customer immediately. They can therefore begin to use their cards more swiftly – driving earlier card activation while increasing activation rates. The issuing provider gets a happy and content customer. Significantly they also benefit from the customer generating revenue (almost) from the minute they receive their card.

Helping to clarify the underlying value of the 'missed' 2 and 3 business days while cards are in the postal system, the table below highlights annual and daily values of card transactions.

Table 1: Transaction per card in US dollars (USD)

Region	Per year	Per day
World	1,136.24	3.11
Asia Pacific	536.76	1.47
Australasia	4,623.97	12.67
Eastern Europe	1,699.30	4.66
Latin America	961.47	2.63
Middle East and Africa	1,486.41	4.07
North America	1,837.53	5.03
Western Europe	3,017.87	8.27

Research Sources:
Consumer Finance: Euromonitor from trade sources/national statistics
Date Exported (GMT): 23/07/2012 09:52:10

Credit card spend is, of course, a key driver of credit card profitability. Credit card issuers receive 'interchange revenue' – the small percentage of spend on each card. According to Vectis, interchange revenue is typically up to 0.5%. The more the credit card is used, the greater the revenue to the bank.

The following calculation models a scenario for an example bank in Western Europe.

Example calculation 1: 'Extra usage days' (a bank in Western Europe)

Number of PIN codes issued	500,000 per year
Transactions per year, per card	8.3USD
Interchange fee	0.5%
Time saving to deliver the PIN code	3 days
Extra Interchange revenue per year *(3 x 0.5% x 8.3 x 500,000)*	60,000 USD per year

- For every 500,000 PIN codes distributed by SMS, an issuer would enjoy 60,000 USD additional revenue per year.

3.1.2. PIN reminder

The PIN by SMS reminder offers the same benefits as those of an initial PIN issuance – speed, convenience and revenue generation. It also offers something less tangible, but potentially just as valuable. The service is so compelling for end customers precisely because it offers rapid support for those who have forgotten their PIN as they try to retrieve money or make a purchase (now many shops no longer offer the option to sign). Customers who need to access their money quickly can ask for their PIN and obtain it immediately, rather than wait for the mail. This encourages a very significant boost in customer loyalty.

In addition, PIN reminder raises card activation rates while reducing customer attrition after a PIN has been forgotten in cases of less/low frequent PIN usage. This flows into reduced dormant cards and accounts, and again becomes the catalyst for increased transactions and card usage.

In the UK, for example, 5% of cardholders report not having used at least one of their cards during the last 6 months because they have forgotten its corresponding PIN, according to a 2012 end-user survey by Gemalto.

The following customer model shows the calculation of an example bank in Western Europe.

In this following model the estimate is based figures from SPA membership showing an average of 7% of the total cardholder base requesting a PIN reminder every year from 'EMV & PIN' card issuers.

- **Example calculation 2: 'Extra revenue from PIN reminder by SMS'**

Number of cards in field	5,000,000
Av. bank income per card, per year *(0,5% interchange fee of approx. 3.017 USD yearly card spend)*	15 USD
Non-dormant card increase *(resulting from reminder of PIN by SMS)*	1%
Extra revenue (5,000,000 x 1% x 15 USD)	750,000 USD per year

- For every 5 million card issued PIN code reminders by SMS, an issuer would enjoy 750.000 USD additional revenue per year.

3.2. Reduces cost of traditional PIN mailer

PIN by SMS distribution not only reduces the time delay of conventional paper-based PIN delivery but also reduces the high costs associated with traditional PIN management, by:

- eliminating paper printing costs for the PIN mailers (using special paper)
- reducing costs associated with sending PIN mailers through postal services

Cost reduction is always attractive in business, but even more so for those financial institutions forced to deliver PINs to a very large customer base. Thanks to economies of scale electronic delivery can be much more cost effective than a paper-based process. With the infrastructure in place, the number of PINs can increase substantially without a corresponding rise in costs.

Furthermore, the traditional process flow after a payment card is requested often corresponds to the automatic PIN issuance and subsequent printing/sending procedure. PIN by SMS lowers the issues and underlying costs related to the issuance of PINs for cards that will never be finally applied for, or indeed used.

3.3. Improves customer convenience

PIN by SMS distribution is an effective way to enhance the relationship with the end user; it's very user-friendly and gets high marks in the convenience stakes. Having the PIN on the phone eliminates that inconvenient and time-consuming trip to the branch, and the long and frustrating wait for the post.

- Customers can get their PINs wherever they are
- Customer can access their PINs at any time (24X7).

This customer convenience is significant because, according to current surveys, banking dissatisfaction remains a critical issue. Approximately 11% of consumers, surveyed in March 2012 by Javelin Strategy & Research, indicated they were at risk of switching primary financial institutions in the coming year.

This data shows the value in investing in user convenience services - from ATM networks, online banking, and increasingly, mobile banking. Receiving a PIN by SMS continues this customer-centric approach for the simple reason that 'convenience trumps fees'.

SPA recommendation: PIN by SMS can be perceived (and positioned as) as being of major benefit to the consumer - increasing customer retention and driving greater loyalty.

3.4. Enables differentiation

In an increasingly connected world, many end users prefer to receive their information through digital channels. PIN by SMS supports the bank in meeting this need and allows the institution to position itself as a true 'new technology' customer champion – offering those new early stage services that extend levels of service and convenience.

In an environment where opportunities are increasingly shifting from product to distribution, several structural factors justify efforts to pursue a multichannel agenda:

- growing client acceptance and appetite for multichannel banking - across a wide range of age groups and income levels
- more and more representatives of 'Generation Y' – those who typically use a wider variety of channels - are now beginning to use banking services
- the opportunity to differentiate from competitors and the need to improve the client experience remain genuine challenges.

SPA recommendation: PIN by SMS distribution is a great way for banks to differentiate their services - offering modern and convenient communication channels to their customers. In addition, by offering this kind of service, the financial institution can drive customer behaviour towards more mobile channels.

3.5. Mitigates risks of traditional PIN mailer

The traditional paper-based PIN delivery channel has failed notably in a number of critical areas. PIN mailers can easily be intercepted en route, along with the card, resulting in fraudulent actions on the card.

The typical risk mitigation factor for postal distribution is to force a delay between the introduction of a card and PIN into the postal system. However, the presence of one envelop in the postal service will notify the interceptor that the other will follow.

Many financial institutions use costly laser-printed, tamper-evident PIN mailers to transmit PINs in a secure way. Currently deployed PIN mailer technology is subject to weaknesses that can reveal the PIN without tampering.

PIN by SMS distribution provides a separate delivery method for both card and PIN. This eliminates the risk of physical interception of both card and PIN mailer from the same mailbox.

Also, if needed, the delivery process can be instantly stopped by the issuer or the cardholder. Depending on the processes in place, the issuer gains control of the entire PIN delivery process. In addition, PIN by SMS allows more simplified reporting and tracking of the PIN delivery process.

In contrast, when the paper-based PIN is delivered to the postal office this control is gone until final delivery to the cardholder's mail box.

SPA recommendation: In terms of security, no system is perfect; PIN by SMS enables issuers to use separated channels for both card and PIN distribution. Implementation is key for improving the chosen distribution system.

3.6. Reduces environmental footprint

There is a strong trend towards green banking in today's market.

Going paperless not only offers a wonderful opportunity for consumers to simplify their banking by eliminating the wait time to receive their PIN, it also supports the green agenda by cutting down on paper and waste.

Going green also benefits financial institutions; many of whom are committed to becoming environmentally friendly through their own CSR initiatives.

A survey released from Javelin Strategy & Research found that 57% of consumers expressed an interest in green banking initiatives; and that number appears to be growing.

SPA recommendation: PIN by SMS distribution offers a very attractive proposition for issuers. SPA recommends they consider all the elements detailed within this section when evaluating their opportunities.

4. Use Cases

4.1. Use case 1: Traveller not using PIN often only when travel

Historically, magnetic stripe card users faced acceptance issues while travelling in EMV countries (Europe mainly). This resulted in poor customer experience and generated complaints from high profile customers.

Consequently, certain issuers took the decision to provide a worldwide payment card solution to these high profile customers. This solution was based on EMV smart cards, using the conventional magnetic stripe with online PIN for domestic payments and EMV features with offline PIN for international payments when necessary.

In order to avoid any further customer experience issues for these clients, this bank decided to offer PIN delivery and PIN reminder service via SMS.

This new enhanced payment product is provided to business and high profile travellers. Prior to departure, the bank informs the cardholder of offline PIN transaction usage. Cardholders can retrieve their offline or online PIN anytime within a very short timeframe. Results suggest this service has increased card usage abroad.

SPA recommendation: Issuers in early EMV migration stage (such as US, MEA and others...) should encourage PIN by SMS services from the very beginning - even before full EMV migration.

4.2. Use case 2: Credit card migration from signature to PIN

Before migrating to EMV & PIN, credit cardholders were used to signing receipts as a cardholder verification method. Credit card issuers needed to provide an efficient way to remind cardholders of their PIN code when required.

The most appropriate solution was to distribute PIN by SMS. Cardholder can call the helpdesk in a similar manner as if they were requesting a PIN reminder by paper mailer – but they are offered a faster method of delivery.

As the introduction of the PIN did not affect the number of active cardholders, the issuer was able to support a similar number of transactions.

4.3. Use case 3: Moving from postal to PIN by SMS issuance at first card issuance

A debit and credit card issuer is searching for a way to deliver PINs out to its cardholders in a faster and more secure manner. Historically the financial institution had always produced paper PIN mailers and used their national postal service to deliver these out to the cardholder's home address.

The use of local postal distribution was characterised by delayed dispatched and 'unconfirmed' delivery that may have been convenient for the postal service, but certainly was not for the cardholder.

The introduction of a PIN by SMS service immediately reduced the time taken to deliver a card and PIN to a new cardholder – in some cases by 3 to 5 days.

From a security standpoint the issuer automatically receives a proof of PIN delivery notification, and the ability to deliver a card and PIN across different channels significantly reduces the chance of interception.

PIN by SMS also offers the issuer the opportunity to monitor cardholder behaviour and provides a rich source of management information not otherwise easily accessible. Activation rates are very important and should a cardholder fail to retrieve their PINs within the given window of opportunity, the issuer can use this information to draw particular conclusions about the customer's intentions to use the card.

SPA recommendation: The PIN by SMS service can include a SMS sent to cardholders informing them that a card has been dispatched and will be delivered soon. In order to do this it is recommended that the provider of the PIN by SMS service is also the provider of card personalisation.

4.4. Use case 5: Cross border PIN delivery

An issuer currently ships thousands of PIN mailers to cardholders across multiple countries - via an international courier - from a centralised PIN mailer production facility. A PIN by SMS service was investigated in order to streamline this distribution process.

In addition to the benefits of increased security and cardholder convenience, eliminating the shipment costs of the physical PIN mailer has been significant. Furthermore, by introducing a PIN by SMS service utilising a central processing model the issuer can now consider centralising PIN issuance processes on a regional, or even global, level.

SPA recommendation: In order for an issuer to build a centralised processing model, a provider of PIN by SMS service needs to have regional or global reach. This is achieved by the establishment of a SMS gateway in partnership with an SMS aggregator able to offer extensive international coverage.

4.5. Use case 6: Emergency cards

Due to intense competition between financial institutions this bank wanted to position itself as a customer-centric organisation – able to rapidly respond to client needs in cases such as emergency card replacement (due to lost or stolen cards).

The bank decided to distribute the PIN by SMS instead of sending paper PIN mailers. Customers who lose their cards simply call into the existing call centre hotline ask for a replacement card as always. A PIN by SMS would then be sent out to the previously defined mobile number.

Now customers do not have to wait the additional two to three working days for the PIN mailer to arrive by post. The new enhanced emergency card replacement procedure also reduces time, costs, and eliminates the risks of receiving the PIN in the mail.

The bank benefits now that customers can use their new emergency cards faster, and customer churn is reduced.

SPA recommendation: Management time and effort spent on new PINs for emergency cards is significantly reduced and the bank can position itself as an innovative and customer-reactive organisation.

4.6. Use Case 7: PIN Issuance at Branch Replacement

Some issuers use in branch processes to deliver the PIN in person to the cardholder at one of their bank branches.

PIN by SMS was looked to as a method to increase the efficiency of its bank branch network day to day activity.

Via a PIN by SMS service the operation to issue PINs via the branch has been eliminated enabling the issuer to achieve efficiency savings allowing the branch network to focus on service provision.

A cardholder benefit was also achieved. As opposed to the cardholder being forced to travel to a branch location they are able to retrieve their PIN from a location of their choosing. As well as greater convenience the PIN by SMS service has enabled cardholders to obtain their PIN quicker having obvious benefits on card usage.

The original rationale for PIN issuance from the branch was, for security reasons, to ensure the card and PIN were delivered to the cardholder via separate channels.

A PIN by SMS service has allowed the issuer to maintain this whilst achieving substantial efficiency and convenience benefits.

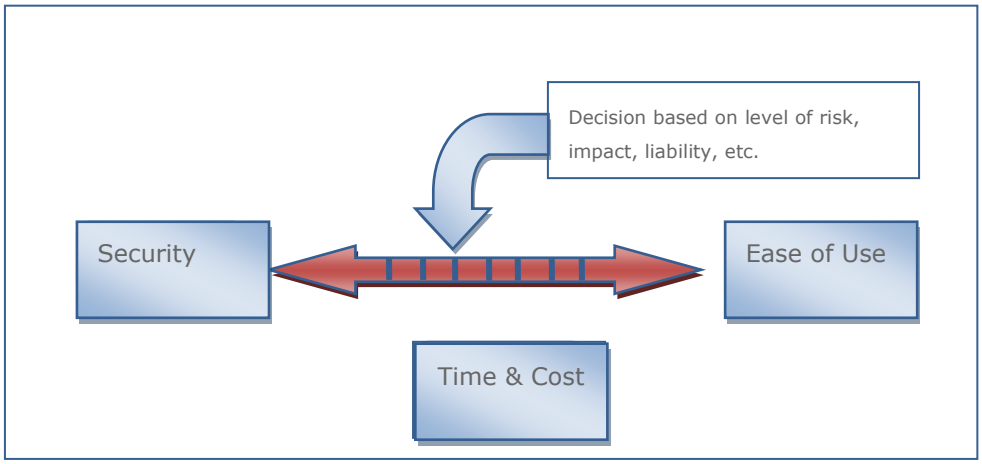
5. About implementations

5.1. Implementation Challenges

Despite growing interest and increasing comfort levels on the part of consumers towards transactions via mobile phone, security and privacy remain key concerns. While the specific issues change with each published survey, there is little doubt that unaddressed concerns will stifle mass market adoption of a PIN by SMS service.

Implementation of any kind of mobile service must place security high on the agenda. However, there is no getting away from the fact that this also represents a complex technical challenge, regardless of the system. Security cannot be simply addressed once then forgotten. At its fundamental level security remains a trade-off between ease of use, user and data protection and cost.

Chart 2: The trade-off between time, cost, ease of use, and security



Given this trade-off, it is necessary to evaluate the proper level of investment in security for each individual case and find a balance.

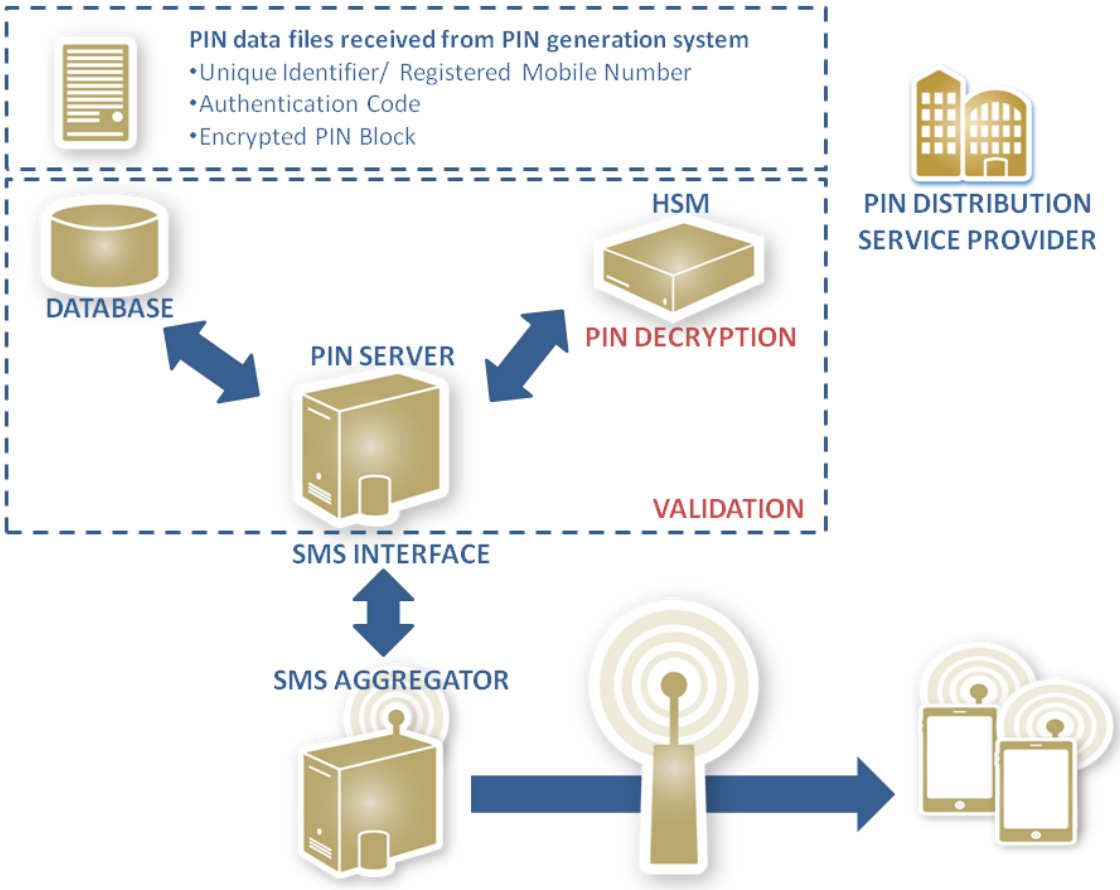
The second major challenge for implementing this type of service is the need to serve a broad range of consumers in order to gain broad acceptance of the solution in the market. The implemented solution must be scalable, which itself poses very particular challenges due to the explosive nature of mobile phone and application adoption.

In this context PIN by SMS distribution is ideal – it is operating system and device agnostic.

SPA recommendation: To leverage the described benefits in section 3 a PIN by SMS solution must be carefully planned and implemented to manage all possible eventualities - from incorrect usage by the cardholder, through protection against suspicious activity to effective incident response. Current implementations by SPA members demonstrate that the right balance is achieved.

5.2. Distribution Overview

Chart 3: The PIN by SMS Distribution System



The corresponding distribution flow for card issuance via PIN by SMS is as follows:

1) Cardholder/customer applies for a payment card. An authentication code is defined.
2) PIN value is generated.
3) The bank adds the authentication code and a unique identifier to the current PIN value and forwards to PIN distribution system.
4) PIN data is encrypted and stored in a Secure Environment (SE) in the PIN distribution system.
5) Card is personalised and packaged for distribution.

6) Cardholder is instructed on how to use the service. These could be instructions printed on the card carrier or by SMS.
7) On receiving the card the customer sends an authentication code to a given number.
8) The PIN by SMS system will validate both the unique identifier and the authentication code. Should both match, the PIN will be decrypted and sent back to the customer via an SMS Gateway.
9) The PIN by SMS system will track delivery and the number of times the customer uses the service.

NB: for the PIN Reminder process, steps 5 and 6 do not apply. Step 1 will also change as cardholder will need to contact the bank for PIN reminder.

SPA recommendation: It is vital to correctly decide the nature of the authentication code. The bank will have to balance between the convenience of information that is well known to the end user and the complexity of using a unique password generated for each PIN by SMS distribution. Furthermore, the cardholder should be allowed to opt-in to the service. It is recommended to leverage the fact that the PIN is already transmitted to the personaliser to minimize the impact of implementation. The service must be highly available and support 24/7/365 cardholder expectation. It should also ensure fast transfer and provide SMS delivery reports (to the handset).

6. Regulatory environment

6.1. Standards

There are multiple standards and guidelines applicable to PIN. The most relevant are detailed below.

- ISO 9564 defines format and encryption of PIN in the context of payment transactions. This standard can be useful to implement a PIN by SMS system when it deals with the format and encryption of the PIN block - but it does not discuss the distribution towards the cardholder.

- PCI-DSS is well known in the payment industry. It was created to increase control over cardholder data in the context of payment transactions. PIN management security is discussed in this standard but only in the context of the payment transaction. Therefore, this standard does not cover PIN distribution.

- FIPS 140-2 Level 3 will discuss the accreditation of cryptographic modules, also called HSM (Hardware Security Module). In some guidelines or requirements applicable to PIN by SMS it is sometimes referred to as the standard for implementation.

- Most payment schemes have defined guidelines or requirements regarding PIN distribution. But in many cases those requirements were written years ago – with the assumption that the PIN will be distributed on a mailer. In this case these requirements are not applicable.

- Some payment schemes have revised existing guidelines to include new requirements applicable to PIN distribution by electronic channels. Some payment schemes also refer to those requirements as part of their vendor certification process.

SPA recommendation: Caution should be exercised when referring to standards: in some cases PIN distribution is not covered while in others they were written some time ago (under the assumption that PIN would remain printed on a PIN mailer).

6.2. Regulations and rules – PIN by SMS issuance

One of the most important rules is the separation of the PIN generation system and the PIN by SMS distribution system. This means that those two systems must be located in separate logical environments, or even in separate physical facilities.

Another rule references the segregation of the data. For security reasons the PIN distribution server must contain no information that could allow cardholder identification.

Some standards and guidelines have also defined the need for the PIN to be pulled by the cardholder from the PIN distribution system. Here, some form of cardholder authentication must be undertaken before distributing the PIN by SMS.

SPA recommendation: Technologies and business models are moving fast – keeping pace with changing guidelines can be challenging. The SPA or your local scheme representative can support you.

6.3. Security aspects

6.3.1. PIN production and issuance

PIN by SMS ensures separate distribution channels, and eliminates the risks of distributing the PIN at the same time as the card.

The unique authentication identifier must be different from the Primary Account Number (PAN).

Some associations and banks mandate that the PIN is pulled by the end-user. In order to trigger the pull, the end user will have to provide this authentication code.

The PIN distribution system cannot store both the PAN and the PIN to be distributed in the same database. In current implementations, the most popular unique identifier is the mobile phone number (MSISDN).

A similar set of rules applies between the bank and its customers for paper PIN mailer distribution.

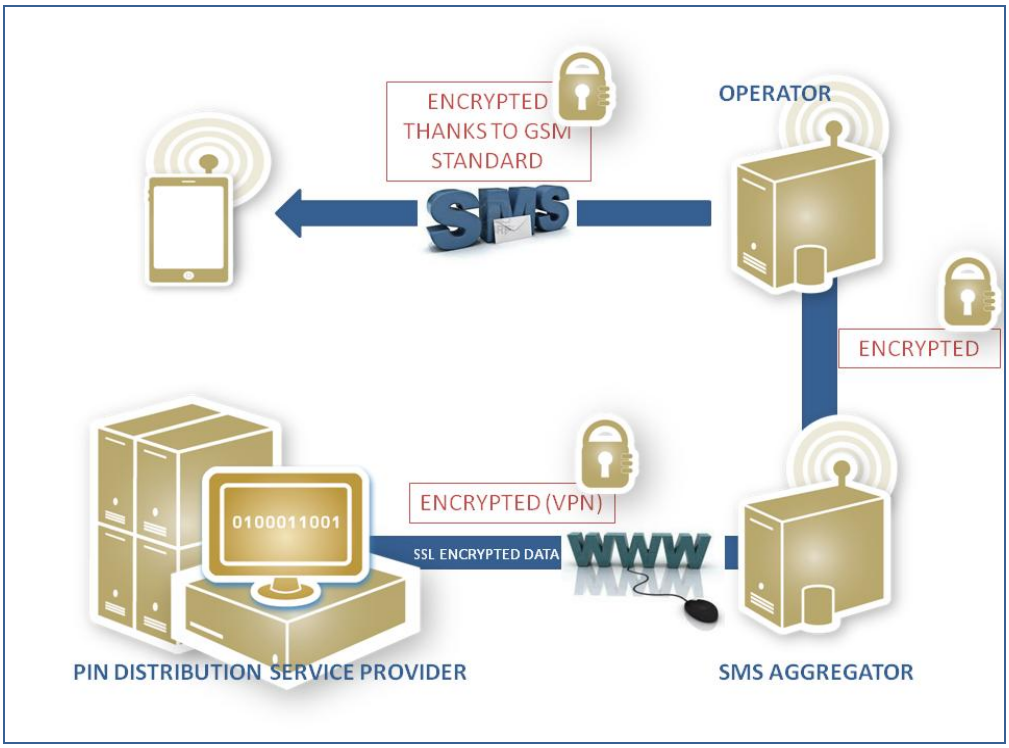
6.3.2. Transmission inside an SMS

The SMS will transit from the PIN by SMS distribution system through an SMS aggregator then a telecom operator, until it reaches the handset.

The SMS aggregator is connected to a large number of telecom operators. A PIN by SMS distribution system will usually connect to this organisation in order to send SMS to all telecom operators.

The telecom operators will distribute SMS to all its subscribers.

Chart 4: Transmission inside an SMS



Is the information enciphered? The SMS aggregator and telecom operators will usually exchange information using a Virtual Private Network (VPN).

How is the security ensured in case of SMS? The security is based on ensuring proper segregation of the data. For example the PIN distribution service provider will make sure that its system does not associate the PIN to any information that would allow identification of the cardholder - such as name, postal address.

What about the MSISDN managed together with a PIN? It will be possible to associate the MSISDN and the PIN code in part of the system. However, none of the different entities would be able to determine who's who due to data segregation. Also, when the SMS is transmitted over the air, it is not associated to the MSISDN of the receiver but to a temporary identifier that cannot be translated into an MSISDN.

SPA recommendation: in order to ensure proper security, the issuer must make sure that its PIN by SMS service provider is able to demonstrate that segregation of data is guaranteed across the complete data flow.

6.3.3. Certification & Guidelines

Most payment associations have created guidelines covering PIN management security. Some associations have also established certification processes for the PIN by SMS distribution system.

Regarding telecommunication, most countries have developed regulations to protect the confidentiality of communication when using electronic channels. In Europe, for example, this is EU Directive 2006/24/CE of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, amending Directive 2002/58/CE.

7. Future outlook and trends

7.1. Mobile phone as convergent device

The mobile phone is rapidly becoming the convergent device of choice for an increasing number of use cases beyond telecommunications; from identification and payment through to online banking and ticketing. This trend can only bring increased security on the handset and across transmission channels.

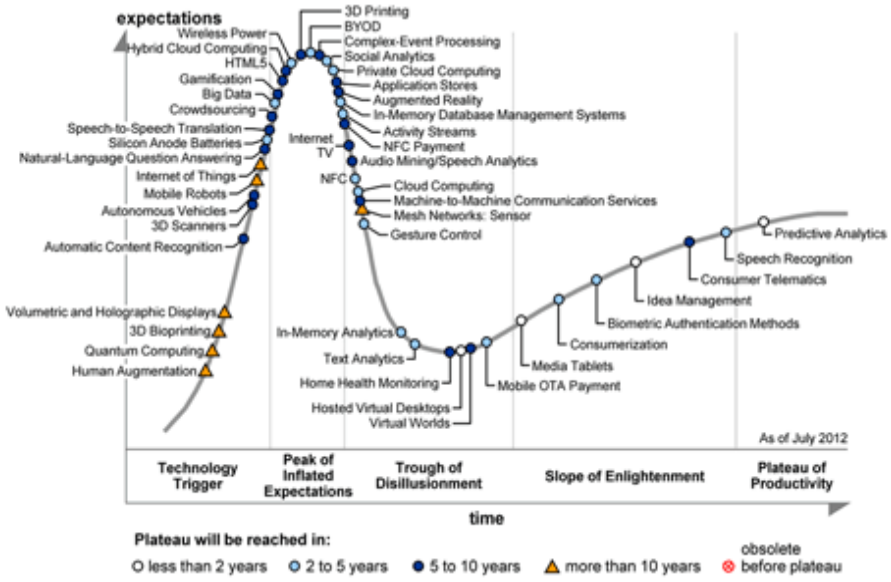
The Hype Cycle for Emerging Technologies report from Gartner, the longest-running annual Hype-Cycle that offers a cross-industry perspective on technologies and trends, highlights a set of technologies that will have broad-ranging impact.

Charting how technologies are built up and adopted, the Hype Cycle concept is rooted in the assumption that technologies follow a basic path of adoption – moving from a trigger point, through overblown hype to cynicism, before finally becoming more mainstream and accepted.

While agreement is very much a matter of perspective, it nevertheless offers an interesting overview of upcoming trends and technologies.

The themes in this year's report – which are of particular relevance to the issues discussed in this paper – include ongoing interest in both the mobile and the Internet of Things. Here, key technologies shaping our increasingly digital world are NFC payment and mobile over-the-air (OTA) payment methods.

Chart 5: Hype Cycle for Emerging Technologies 2012



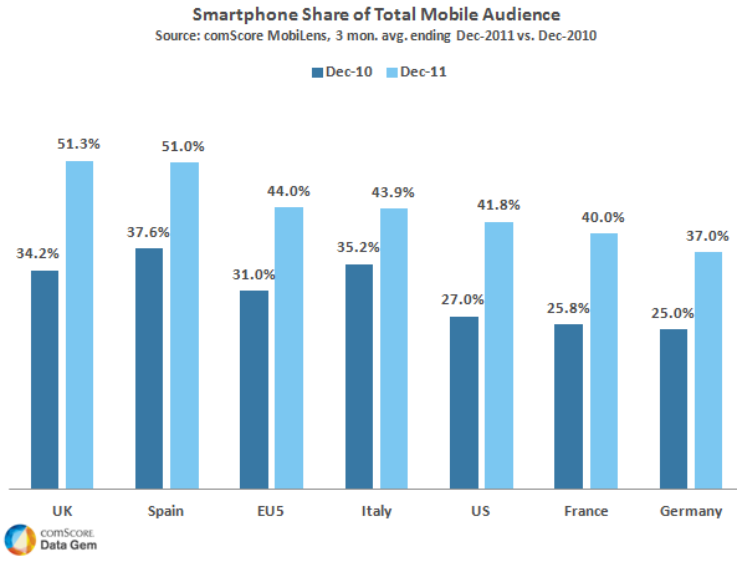
Having crested the curve back in 2011 NFC has moved further down in 2012, and it remains five to ten years away from mainstream adoption. The NFC concept is simple – allowing users to 'swipe' their mobile phones over a compatible reader to make a payment. In a similar way mobile consumers can use their bank card or mobile wallet as a payment instrument, view account activities or top up from their phone.

SPA recommendation: Security is paramount. One of the most decisive future trends is the convergence of communication, financial transactions, identities and mobility. More and more applications are being enabled in the customer's mobile handset while NFC technology is driving the implementation of secure mobile contactless applications (including payment, transit, loyalty and access control).

7.2. Smart phone adoption gains momentum

According to ComScore, smartphone adoption showed strong gains across much of the developed world in 2011. This offers significant opportunity for financial institutions as smartphones combine a host of potential applications and service elements in a single device – from PIN by SMS right the way to advanced mobile banking and NFC proximity payment services.

Chart 6: Smartphone Share of Total Mobile Audience



This explosive growth means customers are now accessing more and more online banking and/or mobile payment services via their sophisticated mobile handsets. And as sophistication increases, so does the security threat, making the new breed of device a target for hackers.

Another important aspect of rising smartphone penetration is revealed by an OS analysis. As of June 2012, mobile data usage shows 65% of global mobile data traffic coming from iOS, 20% from Android, 2% from BlackBerry, 1% from Symbian, and 1% from Windows Phone.

This trend highlights the multiple challenges faced by banks; namely that when it comes to mobile banking these institutions must support multiple platforms and operating systems. Smartphone apps are very appealing and offer tremendous customer engagement and interactivity opportunities. Getting them right (from user interface to the highest levels of security) is critical in ensuring not just service success, but brand awareness and customer retention/acquisition.

Any good app must be compatible with multiple operating system (OS) versions and platforms. But app lifecycles are limited - they must be rapidly improved (often based on social network feedback), and quickly and comprehensively patched. All this locks up development teams into a cumbersome cycle of versioning and development.

An SMS-based solution, on the other hand, will continue to be very effective, and a de-facto platform for multiple services. By using (OS agnostic) SMS technology for user-triggered PIN delivery financial institutions can reach the broadest audience with an offering accessible to all.

7.3. Increasing need for security

As smartphone sophistication and exploding bandwidth drives a new generation of intuitive mobile banking services the need for security is becoming critical in every area of our modern networked lives. Opportunities are emerging to deliver new services. End to end security solutions - from PIN generation and distribution, all the way up to secure storage and even display on the receiving handset – are the next logical steps.

Secure Elements (SE) as tamper-proof hardware (e.g. embedded UICCs, secure micro SD cards or even secure SIM cards) and operating systems on a handset are being increasingly adopted to securely store customer credentials and data.

Another technology push is directed towards expanding the strong security of SEs into the so called trusted execution environment (TEE), e.g. for mobile payment authentication. GlobalPlatform, the organisation which standardises the management of applications on secure smart card technology, has published a white paper that outlines the benefits of introducing and standardising the TEE in mobile devices. The white paper, which is free to download from www.globalplatform.org, will be of interest to all parties operating within the mobile services sector, as the TEE aims to resolve security concerns in the mobile handset market, particularly with reference to digital rights management and finance applications.

The TEE is a secure area that resides in the main processor of the phone and guarantees that sensitive data is stored, processed and protected in a trusted environment. Its ability to offer safe execution of authorised security software, known as trusted applications, enables the TEE to enforce protection, confidentiality, and integrity – as well as delivering the access rights of the data belonging to those trusted applications. This provides end-to-end security.

Providing a secure system environment for IT applications running on mobile devices is crucial to the development and adoption of security-critical applications, especially for smartphones and increasingly for the burgeoning tablet PC marketplace.

8. SPA approach

While the concept of PIN by SMS is delightfully simple, establishing a successful service is subject to a host of issues and complexities; from back end process integration to standardisation and distribution via telecoms partners.

The SPA is here to help banks and other financial service providers understand both these issues and the opportunities, and to provide practical support and guidance throughout the entire process – from programme analysis and design, through product and solution selection to implementation support.

The pace of market change is increasing, requiring institutions to identify and understand these changes and to develop new products and solutions based on the latest technologies.

There are certainly lessons to be learned from other markets and technology deployments, however any attempt to directly transfer these approaches to the PIN by SMS distribution model would be short sighted. We are still in the early phases of adoption. Few organisations have gained first-hand experience or fully understand the specific challenges.

An in-depth knowledge of the industry and a thorough understanding of the available and future enabling technologies are critical elements in helping to deliver success, and to address emerging market issues.

The SPA members are operating on the cutting edge of this dynamic market and actively driving the transformation and convergence process. This is precisely why the membership is able to offer customers the best support, products and solutions.

From the perspective of the emerging PIN by SMS distribution model, it is essential that we all share knowledge and collaborate. This is the purpose of this paper, and we hope the detail included will help financial institutions become better positioned and more prepared for the change. In working together we can ensure costly errors are avoided when selecting how SMS technology for PIN delivery, and that these new programmes will seamlessly integrate with the overall business strategy and processes of today's financial institutions.

9. SPA Recommendations

The SPA believes that PIN by SMS distribution provides very significant benefits for issuers and consumers alike – and the paper's recommendations are outlined below.

In addition, SPA recommends further discussion on this topic with a view to adoption. A thorough analysis of the business case is, of course, critical for each institution, and the SPA and its membership is delighted to support this process.

- Establish a detailed cost/benefit analysis of current paper-based processes
- Analyse your existing regulatory and standards environment, exercising caution as many do not encompass PIN by SMS and engage with a local representative
- Create, with support of the SPA, a financial model to uncover cost savings of PIN by SMS
- Build a defined planning and implementation programme to ensure all eventualities are anticipated and incorporated into solution design, roll-out and operation
- Engage with your domestic telecoms provider to assure a clear telecommunications plan – this may include engaging with an SMS aggregator for cross border operations
- Select appropriate commercial partners to assure the PIN by SMS provider is also the provider of card personalisation
- Take a strategic view of implementation – PIN by SMS can also drive customer behaviour towards existing or emerging mobile banking channels, and can deliver customer-centric branding opportunities
- Contact the SPA at www.smartpaymentassociation.com to support your SMS by PIN planning process

10. Addendum

10.1. Smart Payment Association – a brief portrait

The Smart Payment Association (SPA) is the trade body of the smart payment industry.

The Smart Payment Association addresses the challenges of the evolving payment ecosystem, offering leadership and expert guidance to help its members and their financial institution customers realize the opportunities of smart, secure and personalized payment systems & services both now and for the future.

A non-profit organization founded in 2004, the association now counts six members including the three founding members Giesecke & Devrient, Gemalto and Oberthur Technologies, and Austria Card, Incard* and Morpho.

With more than 898 million smart payment cards delivered by its members in 2011, SPA represents more than 85% of the smart payment cards market. This figure corresponds to a 12% year-on-year growth (2011 vs. 2012), showing the ongoing momentum of EMV deployment.

The SPA works in partnership with global standards bodies, its own vendor community, and an expanding ecosystem of established and emerging brands offering an ever-growing portfolio of advisory and support services.

SPA delivers the market's most accurate barometer of payment trends by publishing an annual analysis of payment trends based on actual manufacturer sales data.

SPA supports the creation and adoption of standards and best practice through an active participation in standards settings organization:

- EPC-CSG/SEPA: Card Representative and Vendor Sector Spokeperson, Chair of the EPC-CSG Task Force to specify the SEPA functional and security requirements for emergent & remote payments (Internet + Mobile), Convenor of the new EPC-CSG Expert Team on Card Innovative Payments, Member of the Preparatory Committee of the SEPA Security Certification Management Body
- EMVCo: Technical Associate and Board Advisor for Card Sector

SPA extends expert advice and support across the payments ecosystem through:

- An eye-growing library of expert technical resources
- Thought leadership collaterals to shape the future of payment

More information on the Smart payment Association (SPA) at www.smartpaymentassociation.com

10.2. Abbreviations and glossary

EMV – Europay MasterCard Visa ▶ Global standard for smart card-based payment transactions, maintained by EMVCo, which is owned by the payment schemes MasterCard, Visa, American Express and JCB.

Issuer ▶ Any mobile NFC payment product, which is a service or application, will be provided by an issuer to the consumer. The issuer for payment products is typically a bank or financial institution. MNOs or system provider can also act as issuer.

Smart card ▶ A smart card is equipped with an additional high-security semiconductor chip. This chip contains an operating system, cryptographic keys and one or more applications, like payment. The chip has multiple security devices to protect against attackers and fraudsters.

SPA - Smart Payment Association ▶ The previous chapter provides an overview of the Smart Payment Association.

PIN ▶ Personal Identification Number.

SMS ▶ Short Message Service. A service that allows the exchange of data between a mobile phone and a PIN server. Typically termed a text message this data can be in SMP or HTT protocol but is common for all SMS enabled handsets.

ATM ▶ Automated Teller Machine. Used by an issuer to automate the dispense of cash to cardholders via self service machines.

POS ▶ Point of Sale Terminal used by retailers to enable payment of goods via a card.

Online PIN ▶ resides in the issuer, or third party, host back end system.

Offline PIN ▶ resides on the chip of the card.

IMSI ▶ International Mobile Suscriber Identifier

PAN ▶ Primary Account Number - 16 digit number on the payment card

MSISDN ▶ Mobile Suscriber Integrated Service Digital Network Number

10.3. Sources

Source	Details
EMVCo	Chart 1: Worldwide EMV Deployment and Adoption in Q4 2011
SPA	2011 Figures Release on 5th March – www.smartpaymentassociation.com
World Bank	
World Tourism Organization (UNWTO)	
Euromonitor	Table 1: Transaction per card in US dollars (USD)
Vectis	
Gemalto	Gemalto end user survey – 18 to 65 years old, user owning a Smartphone and a payment card, 1000 people in France and 1000 people in the UK – April 2012
Javelin Strategy & Research	
Gartner	Hype Cycle for Emerging Technologies 2012
ComScore	