European Parking Industry Payments Landscape

WHITE PAPER

September 2015

Draft V11.8

About this document

In 2011, the European Parking Association (EPA) launched an initiative to assist national associations and their members across Europe in their dealings with the complex world of card or e-payment.

This White Paper seeks to help operators, both public and private, understand the card payment ecosphere: the powerful forces that are at play and the interface between the world of card payments and the technical infrastructure of the parking industry. The Paper addresses new payment methods involving the use of smartphones or other mobile devices. It also addresses the regulatory issues and security concerns facing the industry.

Lastly, the White Paper outlines the case for introducing a standard for the interface between the world of card payments and the parking industry. It briefly describes the IPIPS standard that EPA is promoting and the benefits it would bring to operators.

In most European countries the use of e-payment methods to pay for parking sessions is increasingly rapidly. For parking operators in the majority of the northern European countries, these payment methods now constitute over 50% of their turnover, and in some instances over 80%. There are, however, still a number of countries where the figures are between 5% and 8%. In view of the increase in e-payments in other sectors, notably the retail and leisure sectors, it is highly likely that this trend is going to continue and probably accelerate in the parking sector.

Parking operators are faced with numerous problems and issues when implementing e-payment solutions to support of their operations. They receive advice from various sources: parking equipment suppliers, payment terminals suppliers, payment system providers, each with conflicting interests. They are under pressure from powerful forces: acquiring banks and national or international regulators whose role and purpose are poorly understood. The one thing that is certain is that the interests of the parking operators are not the prime concern of these various parties. This already complex environment is further complicated by the many new entrants who are trying to get a share of the market with “Apps” and the emergence of new ways of paying (such as “in-car”) that may well have a disruptive effect on the parking market. There are an ever increasing number of players and competing technologies in the e-payment sector. This is making it more and more difficult for parking operators to understand what is on offer and to make the right choices and investment decisions.

The European parking sector is a multi-billion euro industry, however, it is composed of a very diverse group of operators. These include a few large national or international companies, a multitude of small and medium sized private organisations and a host of local authorities ranging from those with a few dozen parking spaces to major city authorities with several thousand spaces. This extreme diversity of this group together with the various national peculiarities makes it very difficult for the industry to speak with one voice and more importantly ensure that its voice is heard and its interests are taken into consideration by the powerful forces in the card payment world.

This is a strategically important issue for the parking industry. Operators must work together and federate their efforts across national boundaries to ensure that their voice is heard. The adoption of a standard for parking payments is a very challenging, long term project, it is in the best interests of all European parking operators to ensure that it happens as soon as possible.

Richard Thoma

Keith Williams

Nigel Williams

September 2015

Contents

Part 1 Card Payments

1 The Market

The EPA data collection project[1] provided figures regarding the parking landscape (on-street and off-street) across the European Union. The EPA study estimated that the combined annual turnover of the European parking industry was in the order of 26 billion Euros. A subsequent survey by Visa Europe estimated that figure to be closer to 54 billion Euros.

Whichever figure is correct the parking industry is a significant one in terms of turnover, however, the fragmented nature of the industry makes it difficult to obtain accurate statistical information on the scale of card payments in parking.

As noted in the introduction the use of cards as a payment method varies across countries in the EU. Table 1 illustrates the differences in card stock and usage across the different countries.

Member State	Number of payment cards issued per capita	Number of card transactions per capita	Average value of card transaction per card (€)	Number of POS transactions per card	Annual value of POS transcations per card (€)
Finland	1,45	204	34	141	4 731
Sweden	2,15	185	36	86	3 119
Denmark	1,36	181	45	133	6 008
United Kingdom	2,35	157	59	67	3 929
Estonia	1,33	148	16	111	1 778
Netherlands	1,82	146	40	80	3 160
Luxembourg	3,27	124	74	38	2 810
France	1,27	121	50	95	4 742
Portugal	1,89	117	45	62	2 774
Belgium	1,82	106	55	58	3 164
Ireland	1,32	75	70	57	3 990
Euro Zone average	**1,42**	**65**	**52**	**46**	**2 412**
Slovenia	*1,60*	*58*	*37*	*36*	*1 336*
Latvia	1,13	51	20	45	914
Spain	1,50	48	44	32	1 419
Cyprus	1,52	43	83	28	2 314
Austria	1,31	39	50	30	1 493
Germany	1,60	37	63	23	1 438
Lithunia	1,21	34	18	28	502
Malta	*1,74*	*33*	*74*	*19*	*2 406*
Italy	1,11	29	82	26	2 127
Poland	0,84	27	25	32	779
Czech Repblic	0,93	25	41	27	1 117
Hungary	0,89	24	46	27	1 247
Slovakia	0,98	21	37	21	772
Greece	1,22	6	84	5	418
Romania	0,63	6	37	9	335
Bulgaria	1,07	4	48	4	193
TOTAL EY 27	**1,44**	**72**	**52**	**50**	**2 596**
Source : ECB Payment Statistics, Sept 2012					

Table 1 The Importance of card payments across the EU (sorted by card transactions per capita)

The figures in Table 1 do not include ATM withdrawals. Parking transactions are included in the "Number of POS transactions per card".

[1] Scope of Parking in Europe (Data Collection by the European Parking Association) 2013

It is interesting to note that a number of very well developed economies rank low both in terms of card usage and POS transactions - a clear indication that cash is still the dominant means of payment in these countries.

A recent survey of several of the major European parking operators indicates that, with some exceptions, (eg Spain) card usage in parking facilities reflects the general card use shown in Table 1. For example, card usage as a percentage of all transactions was lowest in Italy (8%) and Germany (12%) and highest in Sweden, the UK and Denmark (60 - 65%). There is also some evidence that the level of card use reflects the general level of parking fees in these countries – lower fees result in a higher percentage of cash payments.

This survey also showed consistent growth in card use across countries between 2012 and 2015. For example in Spain, card use in car parks grew by 4.4% to 56%, while in the same period card use in the UK increased by 9.5% to just over 60%.

2 How Card Payment Works

To understand Card Payments one needs to understand the different elements of the payment process and the agencies involved.

2.1 The Card Payment Landscape

As shown in Figure 1 below, the card payment process involves many types of institution, commercial organisations, regulator and legislators.

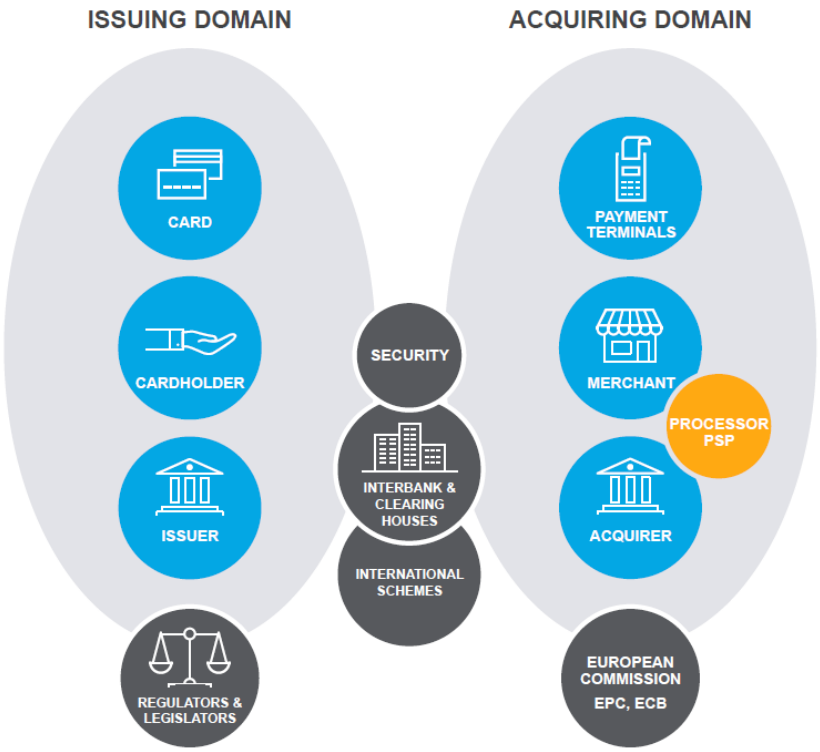


Figure 1 The Card Payment Landscape

The main players in a card payment transaction are:

1. **The Cardholder** – A person (individual acting as a private person or on behalf of a corporate, entity), anyone who possesses a card.
2. **The Issuer** – An institution which issues a card to a cardholder according to a usage contract. The vast majority of cards are issued by banks, but corporate entities (such as telecom companies, retailers, travel and entertainment companies) may also issue cards.
3. **The Merchant** – A person or institution (eg a parking operator) which accepts the card as a payment instrument.
4. **The Acquirer**– An Institution which 'acquires' and processes credit or debit card payments on behalf of a merchant and who guarantees payment to the merchant. Traditionally acquirers have always been banks but some large retailers and oil companies are now undertaking this role. To act as an acquirer within the Single European Payments Area (SEPA), an organization must be a financial institution meeting the Payment Service Directive (PSD) issued by the EU.

Their relationship can be described as a "four party" system. The way this system works and the roles of the other parties shown in the diagram above are described in section 2.5.1, however, to begin we will concentrate on the cards themselves.

2.2 Cards

A card payment involves the use of one of a number of types of card as a payment vehicle rather than cash.

The card serves multiple purposes:

- The card contains the Primary Account Number (PAN) the 16 or 19 digit number on the front of the card.
- It is an identification tool (the identity of the cardholder is confirmed when they use their Personal Identification Number or PIN)
- It is a data support through its magnetic stripe and/or chip. Both must comply with certain characteristics and the chip, in Europe, must be EMV compliant. (See EMV below)
- It is also a transaction support as cards can record some transaction information.

This document does not describe the use of stored value and prepaid card schemes that are specific to locations or operators, but focuses on the schemes that allow a customer to pay with a card that has no direct link to the car park.

2.2.1 Card Types

The main types of card that could be used to pay for parking are:

Credit card: These allow the cardholder to pay for goods and services based on the holder's promise to pay for them. The issuer of the card creates an account and grants a line of credit to the cardholder, from which the cardholder can borrow money for payment to a merchant or as a cash advance. . At the end of the period (usually monthly), the cardholder may repay in full or in part and will accrue interest on the outstanding balance. Most credit cards are issued by or through local banks, but some non-bank financial institutions also offer cards directly to the public.

Charge cards are a specific type of credit card where the issuer creates an account from which the cardholder obtains credit. However the cardholder is required to pay the full balance of the statement amount at the end of the account cycle (usually monthly).

Debit card: When a cardholder makes a purchase using a debit card, funds are withdrawn directly from either the cardholder's bank account, or from the remaining balance on the card. These cards maybe part of a scheme that is specific to the country of issue, or they may be part of an international scheme (eg Visa Debit) that allows international use. Debit cards also often allow the cardholder to access their bank account to withdraw cash etc

Private label card: A merchant-branded credit card that can only be used at that merchant or associated merchants. A private-label credit card is a type of revolving credit plan managed by a bank or commercial finance company for either retail or wholesale manufacturers, such as department and specialty stores. Private label credit cards do not carry a credit card logo such as Visa or Mastercard and cannot be used with other merchants.

Fleet cards are a specific type of private label card used as a payment card most commonly for fuels at petrol stations (eg Allstar, Total GR). Fleet card payments can be managed by similar processes and equipment to those described in this document, but they have some significant differences from credit and debit cards. As with many charge cards, fuel cards use a different processing model.

Figure 2 shows the complexity of card types available.

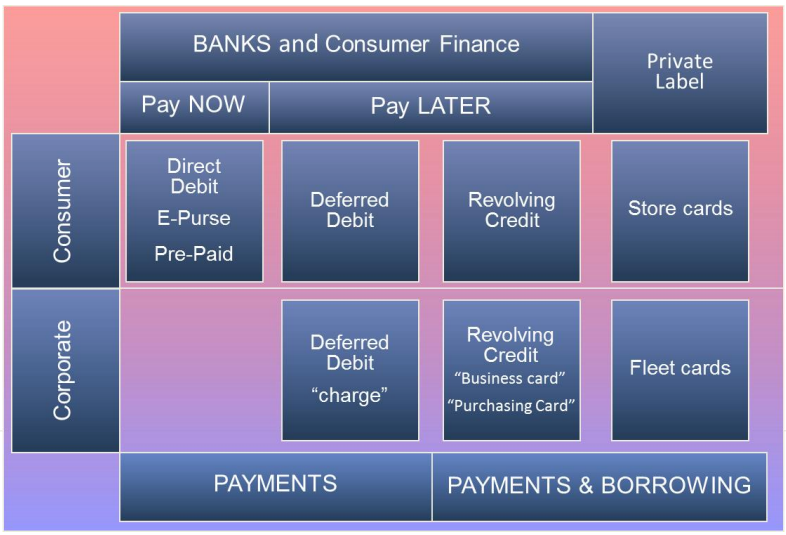


Figure 2 Various types of card (not all cards are bank cards)

2.2.2 Card Characteristics

Within the classification of Credit and Debit cards, issuers may issue cards with varying privileges and value added services (see Figure 3). Cards may also be issued to corporate entities as well as individuals.

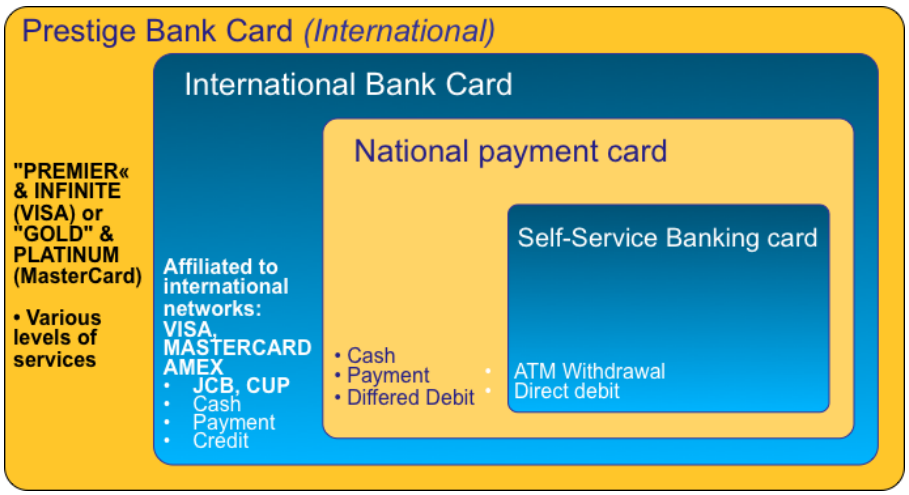


Figure 3 Card issuing and value added services

2.2.2.1 Card Parameters

Card parameters are defined by the schemes to specify the characteristics of a "card instrument". They are then used by the issuing banks to define their commercial offering and used by PSPs and acquiring banks to define which type of processing applies to which card.

A first set of parameters identify the (plastic) card[2]. They are what will distinguish a Visa Infinite credit card from a Maestro debit card.

Each of these parameters is used to recognize the type of card used in the payment and which processing parameters will apply. For example, the interchange charge is different for debit and credit cards.

The second set of parameters defines the types of services attached to the card. For example, a card could be used in any country on any terminal or be limited to some territories and used for withdrawals only.

The limits attached to the card are also important. For example, a card may allow the cardholder to make payments up to €500 per day with a maximum of €2,000 per week, but limit ATM withdrawals to €300 per day and €1,000 per week. These limits also allow activity monitoring of the card and may send some signals that fraud has potentially taken place.

In the case of credit cards, the interest charged for late payment is also an important parameter.

Insurance, medical assistance are often attached to high scale cards and will also be charged to the cardholder.

The lists below summarize the various parameters

- **Products**
  - Brand (Visa, MasterCard, Domestic scheme, Private Label)
  - Type of card (Maestro, Gold, Infinite, co-branded, etc)
  - Visual (colour, pictogram, etc)
  - Technology (stripe, chip [EMV], contactless, biometrics, etc)
- **Services**
  - Territory (national, international – with or without limitations)
  - Limits (daily, weekly limits for withdrawals, payments)
  - Fees, Commissions
  - Acceptance functions (ATM only, Payments, both, cash back, etc)
  - Debit, Deferred debit (the type of card is detected by the payment terminal)
  - Credit
  - Interest (in the case of credit cards)
  - Loyalty scheme
  - Medical Insurance, legal assistance, etc

2.2.3 Co-branding

There are two types of co-branding:

1. Between a scheme (or issuing bank) and a merchant such as Amex linking with KLM/Air France. In many instances this type of co-branding serves a dual purpose, acting as both payment instrument and loyalty scheme.
2. Between an international scheme (e.g. Visa, Maestro) and a national scheme (e.g. Carte Bleue, Bancontact, etc). There are increasing cases as a result of the SEPA initiative which is

[2] Plastic is used to illustrate the concept. Virtual cards may not have the visual characteristics but in all other aspects they must be the same.

demanding interoperability across countries in order to comply with payment "by any card on any terminal".

2.2.4 Card Technologies

2.2.4.1 Magnetic Stripe

Magnetic stripes have been used for data storage on credit cards since the 1970s. The stripe holds the PAN and the expiry date for reading by the payment terminal and may hold other data. Most European cards in circulation have a magnetic stripe and a chip (see below), enabling their use in territories where chip technology has not become widespread.

2.2.4.2 Chip Cards

Chip cards (or IC cards) have a small circuit embedded in the card. When the card is inserted into the reader in the payment terminal, contacts allow the circuit to be read. With many cards it is also possible to write data to the chip. Cards used as credit or debit cards have chips that are EMV compliant. The chip contains an encrypted version of the Personal Identification Number (PIN), leading to the term "Chip and PIN"

2.2.4.3 Contactless Cards

Contactless payment cards contain a second chip and an antenna that enables the card to be read without the need for direct physical contact. There are a number of terms for this technology (Radio Frequency Identification – RFID, Near Field Identification – NFC) Contactless payment cards have to comply with EMV. Transactions using contactless have relatively low limits (€25) although this has been increased in some countries (the UK limit rose to £30 in September 2015) and is likely to be increased further.

2.3 Card Readers (payment terminals)

To be valid a card transaction must be recorded. There is a variety of equipment that achieves this. Payment terminals must be secure and reliable (see sections on EMV and PCI) and are a key part of the payment process. Most devices contain proprietary software and, in an unattended device, have proprietary interfaces to the systems they are embedded into (eg Pay and Display machines). The need to individually integrate each model of payment terminal into a parking system means that it can be difficult to upgrade or exchange different models when, for example, a payment terminal becomes obsolete.

2.3.1 Magnetic Stripe:

These are still common in some territories (eg USA) but are not considered to be secure by most European authorities. However, most card readers in Europe must be capable of reading magnetic stripe cards, as visitors from territories where magnetic stripes are still used have to be able to use their cards. Magnetic stripe readers in current use should conform to PCI standards.

2.3.2 Chip and PIN:

Chip and PIN is now the most common type of reader in Europe. Unattended devices usually consist of a card reader and a separate number keypad (known as a PIN pad). Some devices also use a separate processing unit. These devices must conform to EMV and PCI standards to ensure that card details are read and communicated securely. Visa Europe regulations demand that chip and PIN readers are also capable of reading a magnetic stripe.

2.3.3 Chip Only:

Some vending systems (including parking machines) are allowed under the card scheme rules to use devices where a contact chip reader is used without a pin pad. These are usually subject to a transaction limit (normally approximately €50). Visa Europe regulations for parking demand that a chip only reader must be used in conjunction with a contactless reader.

2.3.4 Contactless Readers

Contactless readers allow a cardholder to 'touch' their card to make a payment. Unattended devices usually have a separate contactless reader. Visa Europe regulations for parking demand that a contactless reader must be used in conjunction with either a chip and PIN, or chip only, reader.

2.4 Card Payment Scenarios

Card payments can take place in a number of ways, depending on the transaction. Payments fall into four basic scenarios:

2.4.1 Card Present

This is the traditional payment scenario in which the customer actually presents his or her card for payment. From a card processing point of view however there is an important distinction between whether the customer is presenting their card to a person or a machine – so called 'attended' or 'unattended'

2.4.1.1 Attended

When the card payment is attended, the person managing the transaction can examine the card to ensure that it is genuine, manage the terminal device to ensure that there are no errors etc. In situations where the PIN cannot be used, an attendant can verify a signature. There are even a few situations where manual card imprinters can still be used!

2.4.1.2 Unattended

Where there is no human available, such as a cashier, to accept a payment, this is known as an unattended environment

When there is no attendant available to manage the card payment device (as is typical in parking), the device must be able to manage all the processes without human intervention. In this environment the machine may be vulnerable to attacks or attempts at fraud. The payment terminal and associated equipment (printer) must also be tamper resistant and provide a degree of privacy for the cardholder entering their PIN.

2.4.2 Card Not Present

This scenario involves the cardholder making a payment, usually to an attendant, at a distance (eg over the phone). This involves risk as there is little evidence of the cardholder's identity or that they have a legitimate right to use the card. To try to mitigate this risk, a merchant will ask for the 'Card Verification Value' number (CVV or CVV2 - also known as the Card Security Code or CSC), which is a separate number printed on the back of the card, as a way to try to confirm that the card is in the possession of the customer. Further checks are possible using the Address Verification Service (AVS), which is supported by the card schemes.

2.4.3 e-Commerce

Online payments are similar to Card Not Present in that the CVV is usually required. However, the online process can also involve other checks (such as whether the cardholder address matches the details held by the card issuer). Most e-commerce transactions in Europe are now backed by a second security process (known as 3-D Secure) that adds an authentication step for e-commerce payments. This is provided by the schemes in association with the card issuers and operates under a card scheme brand name (eg MasterCard SecureCode, Verified by Visa).

Increasingly, credit cards are being used for regular e-Commerce transactions (known as Continuous Payment Authorities) for items such as subscriptions or season passes. In these cases where regular repeat payments are made, the risk of card fraud is much reduced.

2.4.4 Mobile

Much is made of the term 'mobile payment' in many industries including parking. These usually involve making a call or using a smartphone app to make a payment for specific goods or services (eg parking time). Most recently, services such as Apple Pay allow the phone to be used to make a payment in the same way as a contactless card.

It should be recognised that mobile payments are in fact a type of card payment; the cardholder's details are held on file and the app, or service accesses the card details and applies them to the payment. From the merchant's point of view, a mobile payment is simply a card payment (although if the merchant has a commercial relationship with a mobile payment service provider the charging structure may be different)

2.5 The Card Payment Process

2.5.1 Basic Payment Process

As described in section 2.1 a four party transaction involves: the Cardholder (customer), the Issuer, the Merchant and the Acquirer, once the customer has offered to pay the merchant, approval for the transaction is requested from the issuer via the acquirer[3]. Once the transaction is completed, funds are transferred from the customer to the merchant via the issuer and acquirer (see Figure 4).

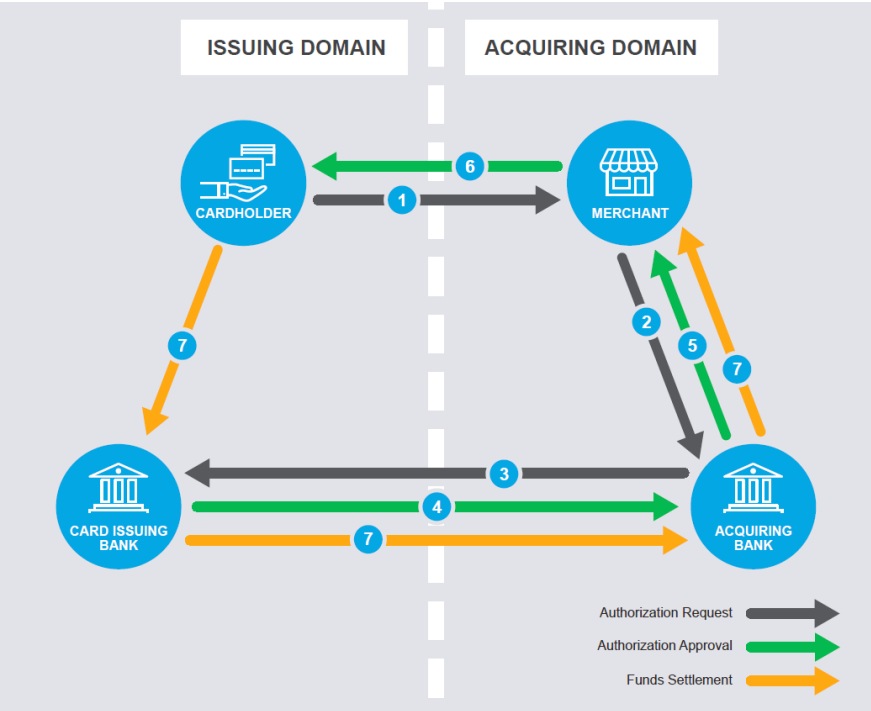


Figure 4 A Four Party Transaction

2.5.2 Other essential parties

In practice, the four party system is an extreme simplification of a complex process, which involves a number of other parties (as described in section 2.1 The Card Payment Landscape):

2.5.2.1 Card Schemes

The four party transaction process requires communication and trust between the issuer and acquirer. Card schemes are payment networks of which a bank or any other eligible financial

[3] There is also a Three Party System (such as American Express), where the function of the issuer and acquirer are effectively combined.

institution can become a member. By becoming a member of the scheme, the member then gets the possibility to issue or acquire cards operating on the network of that card scheme (see Figure 5).

The scheme guarantees the acceptance of the card as a payment instrument between cardholder and merchant through issuers and acquirers[4]. Schemes have a significant role in the card payment process, setting rules and regulations that members must follow (see Card Scheme rules and regulations).

Domestic inter-bank organisations or local clearing and settlement networks.

There are a number of schemes that operate on a national level in countries within Europe (see Figure 8). These are capable of handling payments between their members but are not usually able to operate outside their country of origin.

International Associations

Companies, such as Visa, MasterCard, Union Pay (UP) and JCB are International Associations. These are capable of handling payments within countries or between countries (known as "cross border" transactions).

The Impact of comprehensive EU/SEPA initiatives (see 2.6 below) for standardization of local debit and credit card acceptance ("Any card at any Terminal") and the upcoming reduction of Interchange Fees will lead to a market movement in favour of international schemes (MasterCard, VISA) and their debit card brands (Maestro, V Pay) – resulting in a growth of cross border acquiring business models.

Local debit schemes will experience increased competition from large schemes and their acquirers - this will especially affect the business of German net service providers. The relevant effects of these SEPA initiatives are expected to translate in the issuing of new cards in 2016 and the need for new acceptance solutions from 2017 onwards. In addition, the impact of the reduction in Interchange feeds in the EU from 2016 onwards to the business model of acquirers is not yet clear.

2.5.2.2 Payment service providers (PSP)

PSPs offer technical services to connect merchants to acquirers and can be a key player in the card payment process. In practice this involves providing servers that payment terminals connect to and exchange messages with, as well as reporting services, facilities for making refunds etc. (see Figure 5). Some PSPs will also provide the payment terminals or other hardware. PSPs often connect to more than one acquirer and in some countries will take the role of liaison between the merchant and acquirer.

PSPs will also provide other services for accepting electronic payments by a variety of payment methods aside from credit or debit card, including bank-based payments such as direct debit, bank transfer, and real-time bank transfer based on online banking. Typically, they use a software as a service model and form a single payment gateway for merchants to multiple payment methods. Some PSPs offer other payment related services such as 'closed' card schemes (eg subscription cards) and tokenisation services.

[4] In a three party model, the funds are all managed by a single institution (eg American Express, Discover).

In the parking industry the car park operator often deals only with a PSP and has little or no contact with the rest of the card payment ecosphere.

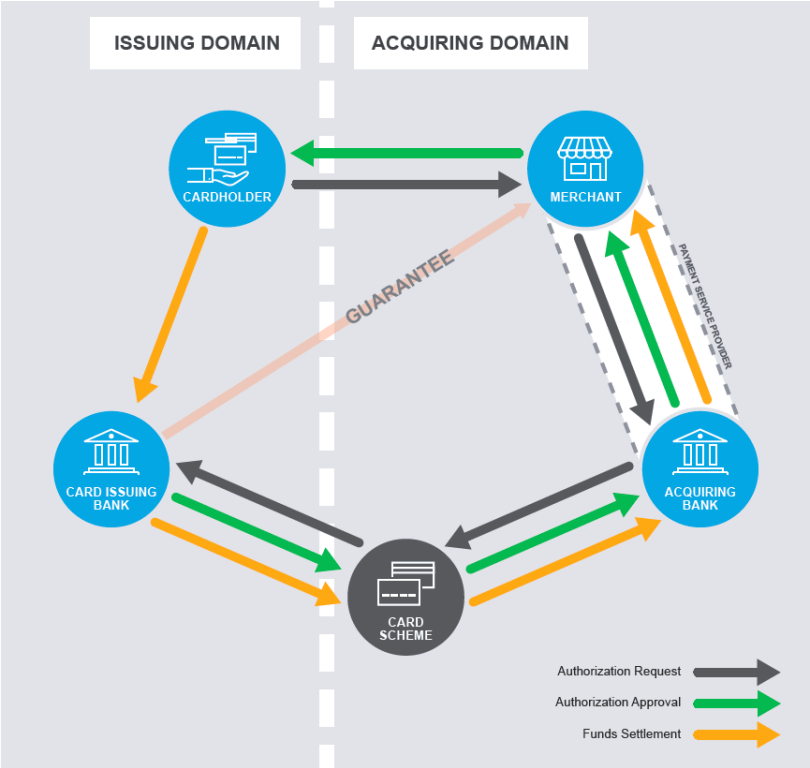


Figure 5 The role of Card Schemes and PSPs

2.5.2.3 Third party processors

A payment processor is a company (often a third party) appointed by a merchant or acquirer to handle transactions from various channels such as credit cards and debit cards for merchant acquiring banks. They are usually broken down into two types: front-end and back-end. Front-end processors have connections to various card associations and supply authorization and settlement services to the merchant banks' merchants. Back-end processors accept settlements from front-end processors and, via the clearing system or central banks move the money from the issuing bank to the merchant bank. These processors are certified and can provide payment services and personalised cards.

2.5.3 The overall process

The card payment process is complex and can involve different combinations of parties depending on the specific circumstances of each payment. Figure 6 illustrates the most common scenarios.

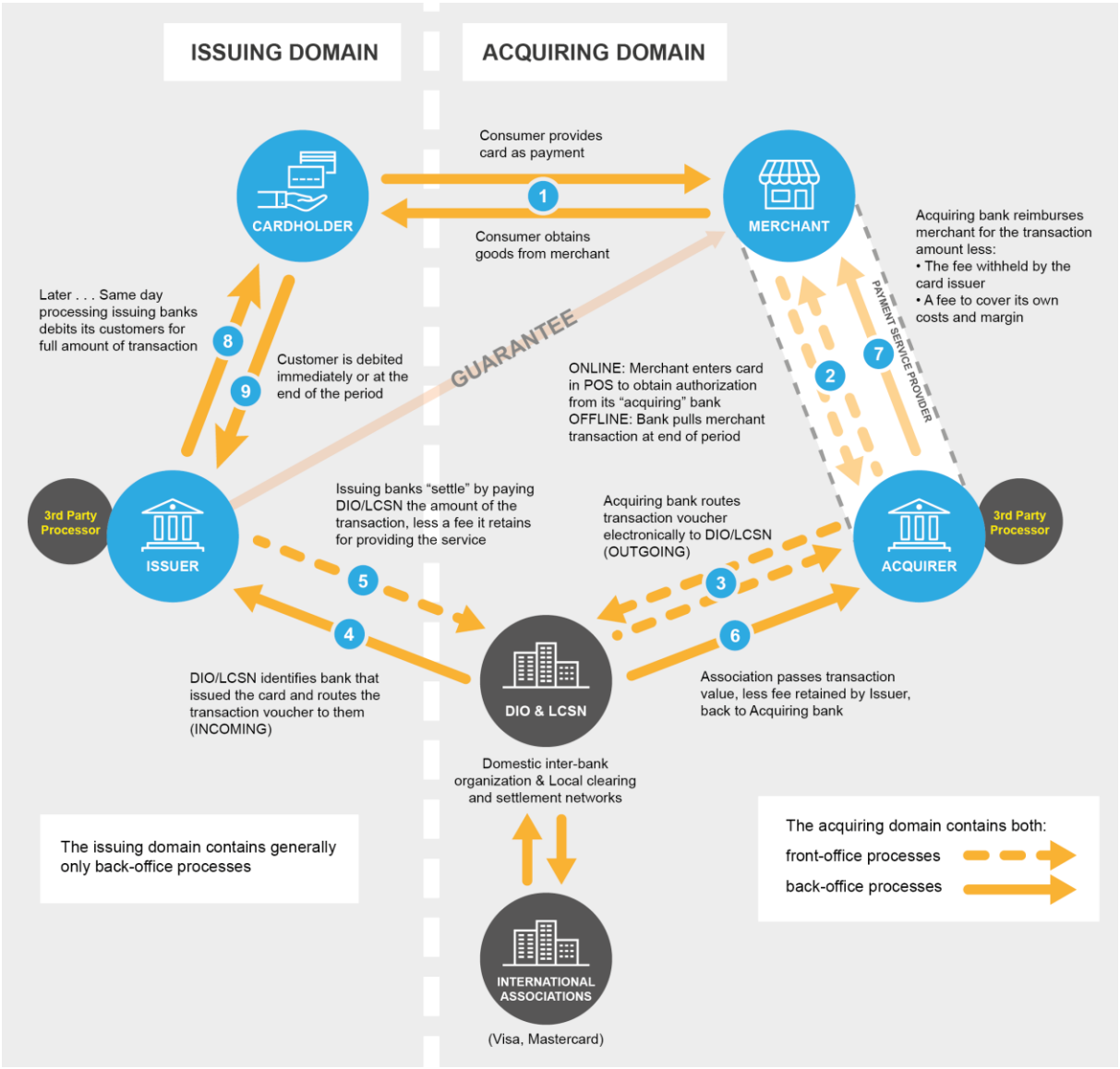


Figure 6 The overall Process

2.5.4 Fees and commissions

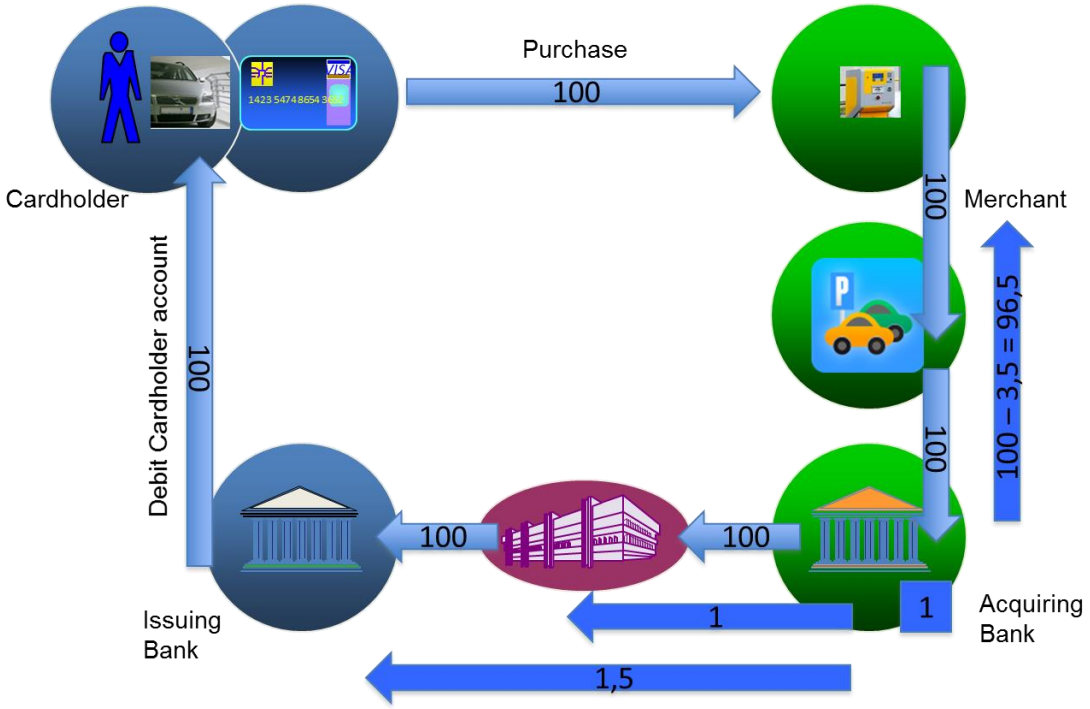
The card payment process is costly, including infrastructure, security, maintenance, regulatory updates twice a year and functional updates to accommodate new services. It is basically funded by fees which are levied by the schemes and redistributed between issuing, acquiring banks and the scheme itself.

2.5.4.1 Merchant Service Charge

Fees are charged to a merchant by the merchant's acquirer for the acquiring service. This covers marketing, selling, support, acquirer risk (fraud, chargebacks, bankruptcy, etc.) and transaction processing fees (see Interchange fees). This is known as the "merchant service charge" (MSC) or so-called "merchant discount rate". The fee is typically 2 to 3 percent of the transaction value and is negotiated, but will vary not only from merchant to merchant, but also from card to card, with business cards and rewards cards generally costing the merchants more to process (which is why some merchants prefer cash, debit cards, or even cheques).

2.5.4.2 Interchange fees

The main subject of contention between schemes, banks and merchants lies in the fees charged for processing card transactions, often referred to as "Interchange fees". The concept of the interchange is illustrated in Figure 7**Error! Reference source not found.**.



The majority of the interchange fee, goes to the issuing bank, but parts of it go to the processing network, the card association (American Express, Visa, MasterCard, etc.), and the merchant's acquirer.

Figure 7 Interchange Concept

The interchange fee generally ranges between 0.1% (debit card) to 3 to 5% (credit cards) depending on the scheme and the merchant's characteristics. It is also interesting to note that countries with low interchange on debit cards have a card payment system largely subsided by national banks.

The majority of the interchange fee, goes to the issuing bank, but parts of it go to the processing network, the card association (American Express, Visa, MasterCard, etc.), and the merchant's acquirer. With a corporate card, the interchange is also often shared by the company in whose name the card is issued as an incentive to use that issuer's card instead of someone else's.

The interchange fee has been under attack by both merchants and governments acting on behalf of the consumer. A recent regulation issued by the European Commission has limited the level of the interchange but this restriction may result in other fees being levied for other parts of the service. It is a fair assumption to expect that the limitations on interchange imposed by the regulators will be compensated by other means.

Costs have to be recovered, if the interchange fee disappears or is reduced too much the whole system may collapse. The challenge is to create a fee structure that is fair to all. Some merchants (in the US) are working on their own payment platform called Merchant Customer Exchange (MCX) to be in a better position to control these costs. They are, however, realizing that their platform infrastructure costs are huge and may negate the expected savings.

A combination of transaction data and acquirer certificates results in the Fee Rule to apply. The factors taken into account are:

- Activity Domain (Bilateral, Domestic, Inter-Country, IntraRegion (e.g. EU) or International)
- Transaction Type (ATM, sales, credit, cash, payment transaction / original credit)
- Card Type and product carte (Consumer, Commercial, etc)
- Card operating mode (revolving credit revolving, deferred debit, direct debit)
- Merchant Category Code
- Clearing timeliness (number of days between transaction date and outgoing date)
- Terminal capability (manual, Stripe reading, EMV, etc)
- POS Entry Mode (track read, track read & sent, chip read, etc)

- Cardholder Identification Method (signature, PIN, etc)
- Authorization present (off-line, on-line, voice, etc)
- Additional data presence (addenda)
- Transaction amount
- Cardholder Presence and Card Presence (MOTO, e-comm, etc)

2.6 The Single Euro Payments Area (SEPA)

The Countries of the EU operate a wide variety of often country specific card schemes as illustrated by Figure 8.

Features of European card systems:

- Multiple "national" card systems
- Diversity of interbank "national" card systems
- VISA and Mastercard are quasi-exclusive schemes on cross border and in some cases "national" operators
- Diversity of business models
- Different legal systems
- Different technical standards
- Transaction volumes are mostly domestic

Figure 8 Card Systems in Europe

The Single Euro Payments Area is the result of a European Union Regulation (SEPA Regulation - EC 260/2012) adopted in 2012, which aimed to create the reality of a European Single Market for retail payments. The introduction of the euro has helped to make cash payments anywhere in the euro area just as easy as at home. But until recently it was not so easy to pay for goods or services electronically in another euro area country, or transfer money from your home bank account to an account in another euro area country, the payment could take much longer, and sometimes the beneficiary did not get the full amount.

The changes brought about by SEPA will make all electronic payments across the euro area – e.g. by credit card, debit card, bank transfer or direct debit – as easy as domestic payments within one country. Other non-Euro countries are also members of SEPA.

Part of the unifying process resulting from the SEPA initiative is the diminishing role of local (national) schemes. There is a movement towards co-branding, enabling a domestic card to be used internationally. Increasingly cards are co-branded, like most of the Girokarte in Germany and the Carte Bleue network (Carte Bancaire) in France. In some countries (Belgium) Maestro has displaced the domestic scheme (Bancontact).

From the payment terminal point of view SEPA has an impact on the fees charged to the merchant. The changes in relative costs of schemes may make some more attractive whilst others (that may up to now have been subsidised) may even disappear.

2.7 Security

2.7.1 Mitigating risk

Whenever there is money involved there is a risk of fraud. Cards (debit or credit) are no exception.

There are many risk areas in card payments including:

- the card (which could be stolen or forged)
- the card transaction itself (which could be tampered with) eg network tapping
- the equipment used (payment terminal, ATM, in parking management system combined with payment terminal)
- the systems that store card information

Today, card fraud is getting more and more sophisticated. It requires expensive equipment and is carried out by criminal organizations. The various recent breaches of large merchants or card processors in computer centres illustrate this trend.

Fraudulent transactions may amount to hundreds of millions of Euros. Some sectors are more vulnerable than others because of their average transaction amount - it is obvious that the very high transaction values at jewellers would be a better target for fraudsters than parking.

Fraud has always been a factor that card schemes and banks have recognized and they have devised and implemented ways to protect themselves and their customers. One early method of protection was to encrypt card data before transmission across a network. The encryption is performed by secured devices (known as Hardware Security Modules) which, using secret keys, encrypt and decrypt the card data.

More security was required however. The chip card appeared first in France and, as it helped reduce the fraud level dramatically, it was picked up by the schemes (Europay, MasterCard and Visa) and developed to become the EMV standard. EMV has evolved since it started in 1996 with more and more complex security algorithms. (EMV is explained in more detail on page 23)

The equipment used in card transaction has also been targeted by techniques such as “skimming”, capturing card data (card number and PIN) in order to make fraudulent purchases often on the Internet. Control of the equipment needs to be regular and systematic to prevent the placement of capturing devices. Sometimes ATM and Point of Sale devices have been tampered with on an industrial scale.

EMV helped but even the security added by the presence of a chip was not enough. Systems where card data are stored became valuable and experienced various attacks. These systems are used by banks, processors and merchants. In order to make fraud attempts more difficult PCI Data Security recommendations have been published by the PCI Standard Security Council and endorsed by the schemes (Visa, Mastercard, Amex, UP, JCB)

Non-compliance with the PCI recommendations will leave the merchant or the processor responsible for the fraud damages that a security breach would entail. Therefore, PCI is taken very seriously by all players. It has a cost and it is evolving all the time but these costs are less than the total amount of fraud that they prevent. An attack on a system that compromises 50 million cards could result in losses of €300 million or more. PCI is explained in more detail in 2.8.2.1 below.

2.7.2 Tokenisation and Encryption

There is also a protection method called tokenization that is becoming more and more important. This is the upcoming trend in security in parking and will facilitate “card-in/card-out” operations and the entry and payment process.

Tokenization and encryption are two fundamentally different technologies.

Tokenization is a technology that creates an index, or token, to a specific piece of data such as a credit card number. The original data value - in this case the card number - is pushed through a mathematically irreversible process that produces a “token.” Tokenization cannot be reversed or broken - it relies on a party to reconcile a token with the original data.

Encryption builds a relationship between the encrypted data and the original data. With encryption, in order to get back to the original data, you must provide the appropriate encryption key. Key management is an essential part of payment platforms.

Tokenization and encryption can coexist. They are not mutually exclusive.

2.8 Standards and Regulation

As part of the international financial services industry, card payment is heavily regulated. This regulation, which can take the form of standards and certification and/or licences to practice, is addressed by a number of bodies that operate at a national, continental or global level, resulting in some parts of the industry having to deal with different groups of regulations in different countries, or being able to operate in one area but not in another.

2.8.1 Regulators and Regulations

2.8.1.1 European Union

There are a number of bodies operating at European level, including the ECB (European Central Bank) and the European Payments Council, as well as the institutions of the EU itself. Much of the regulation that these bodies are involved in relate to SEPA.

Since 2013 the EU has been in the process of updating rules on payment services to improve security, widen consumer choice and keep pace with innovation. These rules, known as the Directive on Payment Services (PSD2), provides the legal foundation for the creation of an EU-wide single market for payments. The PSD aims at establishing a modern and comprehensive set of rules applicable to all payment services in the European Union. The target is to make cross-border payments as easy, efficient and secure as 'national' payments within a Member State. The PSD also seeks to improve competition by opening up payment markets to new entrants, thus fostering greater efficiency and cost-reduction. At the same time the Directive provides the necessary legal platform for the Single Euro Payments Area (SEPA).

2.8.1.2 Central Banks, Financial Service Agencies, National Payment Councils

Most European governments have issued national regulations. Regulators overseeing the financial operations within a country work within international standards and many in the Euro zone are now adopting SEPA based regulations, but very often governments impose their own interpretations.

2.8.1.3 Data Protection

All EU countries have legislation on data protection that implements the EU directive 95/46/EC with regard to the processing of personal data. Implementing the standards listed in this document enables parties to more than meet the data protection requirements of the directive with regard to payments, however merchants must remember that they are responsible for ensuring the security of their customers' personal data.

2.8.2 Standards

2.8.2.1 Payment Card Industry Data Security Standard (PCI)

The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information. Organizations that handle branded payment cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB must comply with the standards. Private label cards – those which aren't part of a major card scheme – are not included in the scope of the PCI DSS.

The PCI Standards are administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is performed annually, either by an external Qualified Security

Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

PCI DSS

PCI Data Security Standard (PCI DSS) provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents.

PCI DSS compliance is required of all entities that store, process, or transmit cardholder data, including financial institutions, merchants and service providers. The PCI DSS applies to all payment channels, including retail, mail/telephone order, and e-commerce. The card scheme's compliance programs manage compliance with the PCI DSS with the required program validation.

The PCI DSS offers a single approach to safeguarding sensitive data for all card brands. It consists of twelve basic requirements categorized as follows:

Control objectives	PCI DSS requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

The PCI DSS standard has been updated a number of times since the first version was published in 2008, each time the standard has been raised.

There are two other standards that are relevant to the parking industry. Each is designed to improve the security of equipment supplied to merchants:

PA-DSS

The **Payment Application Data Security Standard** (PA-DSS) was implemented in an effort to provide the definitive data standard for software vendors that develop payment applications. The standard aims to prevent developed payment applications for third parties from storing prohibited secure data including magnetic stripe, CVV2, or PIN. In that process, the standard also dictates that software vendors develop payment applications that are compliant with PCI DSS.

PCI PIN Transaction Security (PTS)

PCI PTS security requirements reduce the likelihood and limits the potential impact of PIN compromise by establishing the minimum criteria for the design and manufacture of secure Pin Entry Devices (PEDs). The PCI PTS security requirements apply to Point of Sale (POS) devices and Encrypting PIN Pads (EPPs) used in unattended situations (such as parking machines). The PCI PTS standards are reviewed and updated every three years.

2.8.2.2 EMV

The EMV Integrated Circuit Card Specifications for Payment Systems describe the requirements for interoperability between chip based consumer payment applications (such as cards) and acceptance terminals to enable payment. It is named after its original members; Europay, MasterCard and Visa.

The specifications are managed by EMVCo, global organisation with six member organisations—American Express, Discover, JCB, MasterCard, UnionPay, and Visa—and is supported by large number of banks, merchants, processors, vendors and other industry stakeholders who participate as EMVCo Associates.

The distinguishing feature of EMV is that the consumer payment application is resident in a secure chip that is embedded in a plastic payment card, often referred to as a chip card or smart card, or in a personal device such as a mobile phone. The chip provides three key elements:

- it can store information;
- it can perform processing;
- It is able to store secret information securely, and perform cryptographic processing.

In order to execute a payment, the chip must connect to a chip reader in an acceptance terminal. There are two possible means by which this physical connection may be made which are often referred to as contact or contactless. With contact, the chip must come into physical contact with the chip reader for the payment transaction to occur. With contactless, the chip must come within sufficient proximity of the reader, (a maximum of 4cm), for information to flow between the chip and the acceptance terminal. In both scenarios, the acceptance terminal provides power to the chip to enable the chip to process.

Chips that are embedded in form factors such as plastic payment cards may support only a contact interface, only a contactless interface, or both contact and contactless. Chip cards that support both contact and contactless interfaces are referred to as dual interface. When the chip is installed inside a non-card form factor, such as a mobile phone, contactless is typically the only option for connection to the acceptance terminal.

EMV is designed to significantly improve the security for consumer card payments by providing enabling features for reducing fraudulent payment that results from counterfeit and lost and stolen cards.

The features that are defined by EMV are:

1. Authentication of the chip card to verify that the card is genuine so as to protect against counterfeit fraud for both online authorised transactions and offline transactions.
2. *Risk management parameters* to define the conditions under which the issuer will permit the chip card to be used and force transactions online for authorisation under certain conditions such as offline limits being exceeded.
3. Digitally signing payment data for *transaction integrity*.
4. More robust *cardholder verification* to protect against lost and stolen card fraud for EMV transactions.

Counterfeit and lost and stolen card fraud represents significant cost to all participants in the payment process, including retailers, acquiring banks, card issuers and cardholders. Costs are realised through the processing of cardholder disputes, research into suspect transactions, replacement of cards that have been counterfeited or reported as lost and stolen, and eventual liability for the fraudulent payment itself.

The PIN verification process is described in Figure 9.

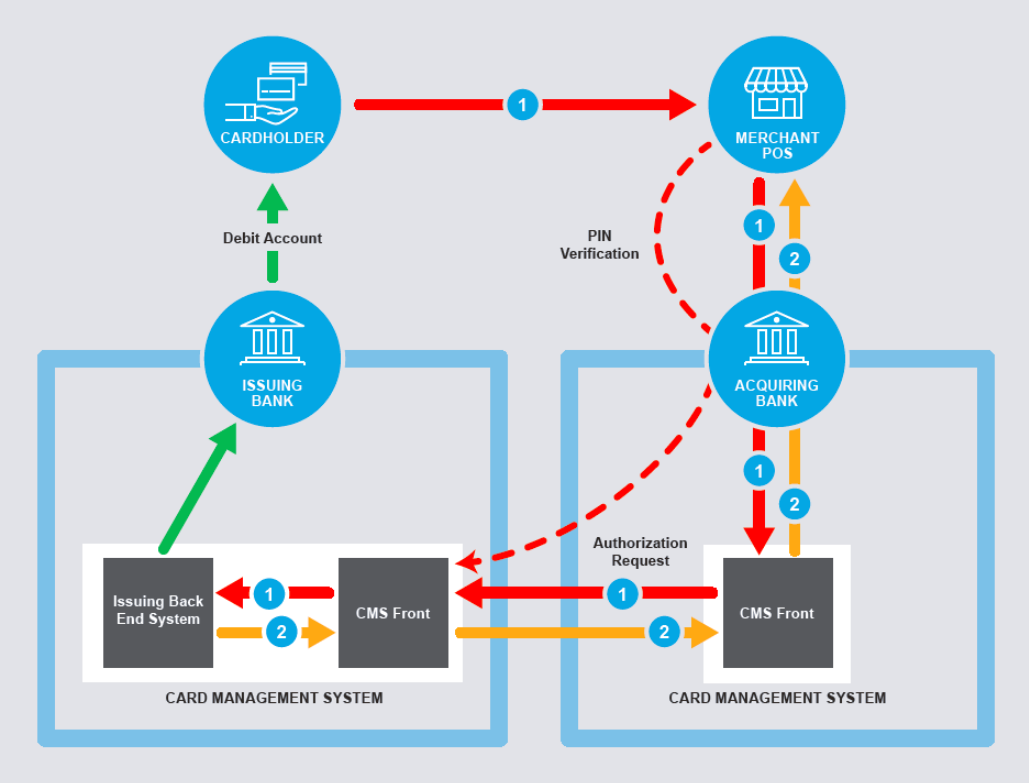


Figure 9 PIN Verification Process

Note: CMS Front is a Front End Processor that accepts the incoming transactions from the merchants and routes them to the issuing banks for authorization. In the case where the acquiring bank is also an issuing bank, its Card Management system will process the transaction internally. This is called an "ON-US" transaction.

The entire process is protected by encrypting the card data while transporting the transaction over the network. Encrypting devices are a crucial element of the card infrastructure. As no card data (card number, name of cardholder, etc.) should travel in clear over the network, encrypting data protects the customer. As with data protection on the acquirer and issuer sites, it is part of the PCI mandate.

2.8.2.3 International Organization for Standardization (ISO)

Many of the standards that have been developed for payment are registered with the ISO. Standards cover all aspects of the card payment industry including communication protocols and equipment specifications.

2.8.2.4 Card Scheme rules and regulations

All the card schemes issue rules that members must comply with. Visa Europe publishes the 'Visa Europe Operating Regulations', whilst Mastercard publishes the 'MasterCard Rules', which has sections specific to Europe.

These rules are very detailed and cover all aspects of the card payment process, including the equipment types that can be used, the standards that must be met, obligations of each party to the others, etc. The rules also require that members meet the EMV and PCI standards (including obtaining certification where appropriate). The schemes will sometimes allow variances to a rule,

usually for a specific technical or commercial reason. The rules and regulations for each card scheme are updated regularly.

3 New Payment vehicles

There are many new proposals for payments:

1. More and more card issuers are providing credit and debit cards with contactless function but the acceptance in contactless readers is trailing.
2. Mobile driven payments. Mobile initiated transactions may be NFC (contactless) if contactless acceptance takes off significantly, but mobile transactions may not need NFC to happen (This will be covered in more detail later)
3. Square, iZettle, MPowa, TechCrunch and others. These promote a mobile card reader that operates in conjunction with a smart phone.
4. Tablet POS which is basically an upgrade of the mobile card reader technology
5. Apple Pay and likes (Google pay, Samsung pay, Android pay)
6. Social media (Facebook credits). The challenge is how it will be regulated as social media sites would need to be financially regulated and provide sufficient security.
7. Wallets (Google, PayPal) These have the advantage of being anonymous and convenient, and are a useful cash replacement. These have the problem of potential susceptibility to crime and money laundering
8. Connected Car integrated payments

On one hand, mobile and web based end-to-end payment offerings from new players (Apple, telecommunication providers, Google, PayPal, Square, etc.) are putting additional pressure on traditional payment industry, on the other hand, the upcoming NFC / QR / BLE payment trends will most likely create an additional window of opportunity for hardware exchange.

Notes on mobile activated payments

The term mobile payment is often incorrectly used. In most cases the mobile phone **is just an enabler**. The payment is still a **card payment.**

Definition of a payment: Payment is a movement of money between two bank accounts: payer's and payee's bank accounts. There are only three (3) ways to make a payment:

- Direct Debit
- Credit Transfer
- Card Payment

Anything else is NOT a payment. For example, Starbuck's mobile payment is NOT a payment. It is only the usage of funds prepaid on an account. The original transaction to fund the account is a payment. The rest are not payments.

A mobile payment standard is being developed but based on EPC work. The IFSF approach is to focus on the message format and thus be agnostic of mobile device, network operators or banks.

Part 2 Standards for Parking Payments

4 Card payment and the parking industry

As outlined in Part 1 the card payment ecosphere is complex. For the sake of simplicity this white paper focusses on "barriered" off-street parking systems, however, the same principles apply to on-street pay and display machines.

Over the past 20 years many of Europe's car parks have been equipped with "barriered" pay on foot systems. The elements of such systems will be familiar to operators (see Figure 10)

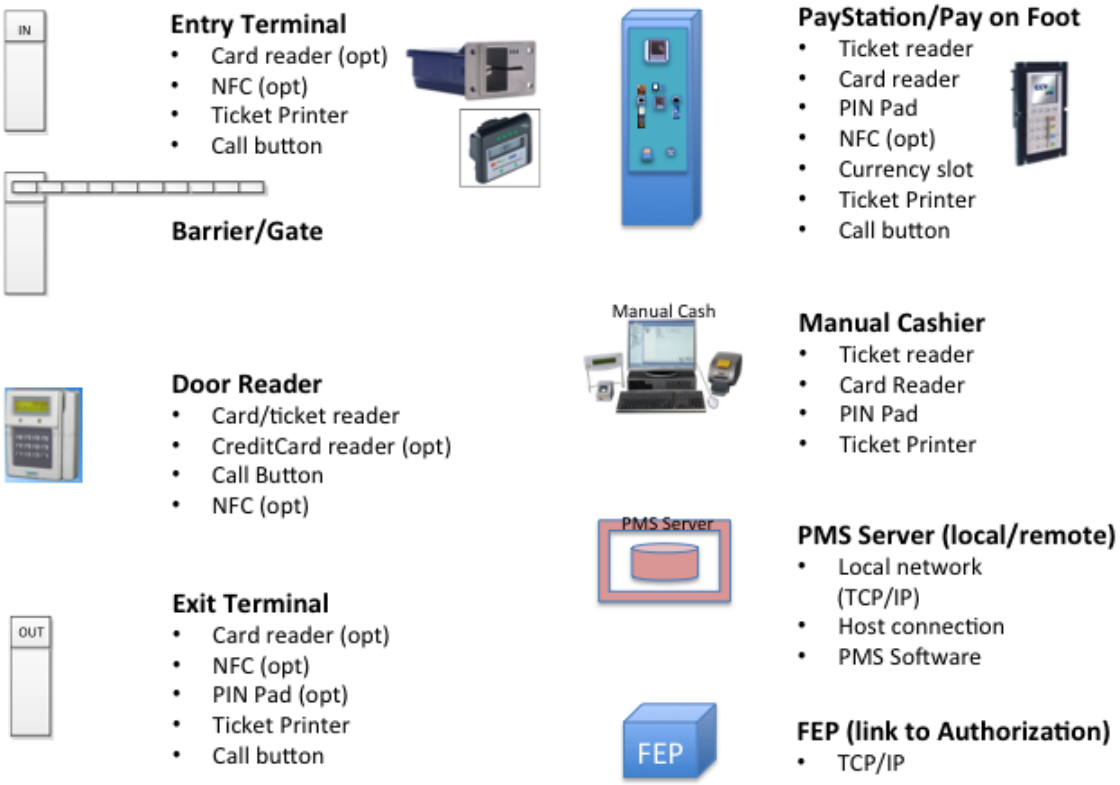


Figure 10 - Elements of a Pay on Foot System

In the simplest scenario the customer enters the car park by taking a ticket from the entry terminal. This ticket starts the parking session and identifies the parker. When the parking session is finished, the customer pays for his or her parking time at the pay station and then drives out of the car park after inserting the paid ticket into the exit terminal. As operators will be aware there are an increasing number of ways that the car/customer can be identified and the parking session started without the customer necessarily taking a ticket (eg ANPR, RFiD tag, etc). One effect of these innovations is that the distinction between the payment process for on-street and off-street parking is becoming less relevant.

An exploration of the different ways that customers can interact with parking equipment is outside of the scope of the present paper. This paper focuses on the interface between the parking equipment and the card payment ecosphere. This interface is formed by the payment terminal (card reader and keypad) in the parking equipment which is used to authorise card payment or alternatively by the App if one is being used to handle the payment of the parking session.

5 Challenges for parking operators

In almost all European countries parking operators are under increasing pressure to offer their customers easy to use e-payment and mobile payment solutions at the lowest possible cost. At the same time operators are worried about investing in new systems and technology. Are they secure and fully compliant? Are they future-proof? Which new services and products will flourish and survive? Which will falter and disappear in a couple of years?

As described in Part 1 the card payment ecosphere is complicated and constantly evolving. It is practically impossible for parking operators to obtain neutral, unbiased and clearly understandable advice on the best way to approach important matters such as:

- Data Security
- Mobile payments and Contactless payments
- Certification of payment terminals lapsing without any viable solution other than changing all the parking equipment

The last point is a particularly important one, in Part 1 there was a brief description of the payment terminals. For operators there are a number of issues with these terminals, most importantly there are a limited number of terminal suppliers, each of whom have different software protocols and in some cases different sized pin pads. The result is that is it very difficult, practically impossible, for operators to change the payment terminals and install another make or model.

Each parking equipment supplier works with a very limited number of terminal suppliers. The same is true of the payment service providers (the companies who provide gateway services to the card payment ecosphere). Thus when operators buy a certain make of parking equipment they are effectively (without necessarily being aware that this is the case) limiting their choice as to which players in the card payment ecosphere they can work with.

This limited choice reduces the operators' ability to negotiate or renegotiate terms for their card processing fees during the life of their parking equipment. In a market where the volumes of card payments in car parks is increasing steadily and the structure of card processing fees and services is changing rapidly, this is clearly a serious handicap for operators who are under pressure to optimise their financial performance.

There is a further problem. Each model of payment terminal has to be certificated before it can be used. This certification is complex and may be valid for a period of up to 6 years (depending on the approvals required). There have been a number of recent cases (eg the Artema in the UK and the Wynid in France) where the certification of the payment terminals is no longer valid due to changes in the regulations (see Payment Card Industry Data Security Standard (PCI) & EMV above) long before the end of the useful life of the parking equipment. In cases where there is no interoperability (ie ability to change the model of payment terminal) the parking operators are then obliged to replace their parking equipment before the end of its useful life.

Lastly, as noted in Part 1, there are an increasing number of innovative ways to pay for goods and services including parking[5]. Equipment suppliers suffer the costs and risks associated with developing innovative solutions to comply with differing standards and certification processes in each European country. The lack of a common standard for the interface between the parking equipment and the payment ecosphere is hampering the introduction of such innovation, resulting in higher development costs and longer time to market for innovative products and services in the parking sector.

[5] It is important to note that when innovations occur there is no certainty on their long term viability. This uncertainty is shared by operators as well as parking equipment suppliers.

6.1 Strategic objectives of the EPA payment initiative:

The strategic objectives are as follows:

- **Provide operators with a good understanding of the card payment process so that they can take informed decisions on the best solutions for their specific requirements**
- **Provide a payment standard (IPIPS) for the industry and promote its adoption by operators and other stakeholders.**
- **Establish EPA as the voice of the European Parking Industry in discussion with the different stakeholders in the card payment ecosphere.**

6.2 The origins of the e-payment initiative

The origins of the EPA e-payment initiative date back to the introduction of Chip and PIN technology in 2007. The task group was led by Sten Åke Håkansson. The group's main objective was to obtain a waiver for the parking sector so that authorisation via a PIN pad was not required for all parking transactions. The group had some success in that Mastercard and Visa agreed to allow a waiver of their rules so that transactions of less than 50€ in the case of Visa and 100€ in the case of Mastercard could be accepted at unattended terminals in car parks without requiring an authorisation by PIN pad.

In 2011 the EPA set-up a new work group. The objectives of this group were to enable parking operators to better understand the payment ecosphere and to work on the issue of standards. The group is composed of representatives of parking operators, equipment suppliers and payment service providers. It is co-chaired by two of the authors of this white paper.

6.3 The agreement with IFSF

To help its members find their way in the e-payment jungle, following detailed research and analysis by the members of the work group, EPA signed a historic agreement in November 2012 with the influential International Forecourt Standards Forum (IFSF). The two organisations agreed to cooperate to simplify electronic payments for motorists paying for fuel and parking by adopting common standards for equipment connectivity and transaction processing.

IFSF is a forum of international petroleum retailers with the common objective of harmonising equipment interconnectivity and communication standards within the petroleum retail business. The IFSF standards have enabled petroleum retailers to process all types of card payments identically in all countries. The IFSF standards have facilitated cross border acquiring contracts and the interconnection of different Point of Sale, Card Terminal and Payment Card systems on a very large scale. The standards are currently being extended to cover all mobile payments and to provide a tokenization standard that will make it possible for the parking industry to have one single "card-in/card-out" operation for customers in every country.

The signature of the agreement with IFSF marked the birth of International Parking Industry Payments Standards - IPIPS (powered by IFSF). It should be noted that the work group had previously considered developing standards specifically for the parking industry, however, it was clear that the parking industry did not have the resources to embark on defining its own standards. The best option would be to select an existing standard which would fit the needs of the parking industry. There were very good reasons to adopt the IFSF standards as:

- IFSF standardization has been in place for almost 30 years in the oil retailers and continues to develop with new technologies (mobile, NFC)
- IFSF standards are implemented in all European countries
- Payments for petrol and parking are not too different

- The petrol industry is more powerful than the parking industry
- IFSF standards are accepted by Visa, MasterCard, EMV, PCI

The EPA work group has 'translated' the IFSF documentation from 'fuel' to 'parking', describing the communication protocols for each part of the payment process, required for the parking industry as well as defining the 5 main parking use cases in order to validate the IFSF standards. Figure 11 below shows a very simplified view of how IPIPS protocols specify the standard links from the parking equipment through to the bank.

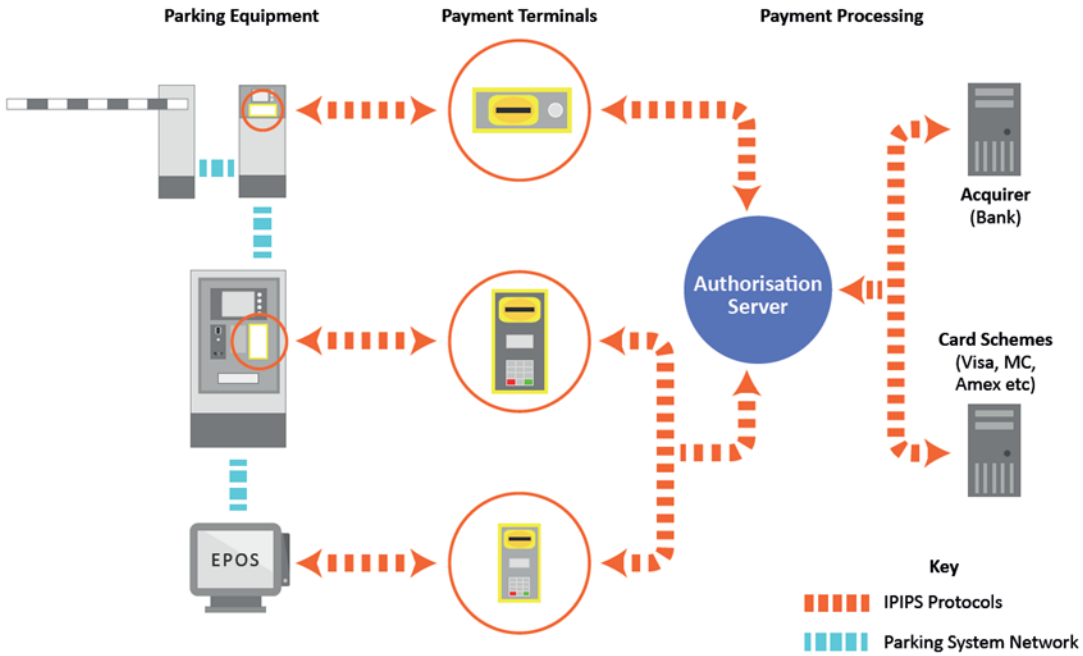


Figure 11 IPIPS protocols link the parking system to card processing

Payment technology is evolving very rapidly and to ensure that we are not left behind, the e-payment Work Group has participated in IFSF initiatives on mobile payment and tokenisation, creating the potential for developing a long term strategic plan for the parking industry.

Mobile payment standardisation will help parking operators to link up with the many smartphone based payment services that are springing up across Europe. Systems that use the standard will be able to accept a payment from any app or phone payment system and apply that payment to a customer.

The introduction of "tokens" (encryption of the card identification to prevent fraud) in the identification and payment process cycles will allow a secure "card-in/card-out" process as well as reservations of parking spaces using credit cards, without the risk of compromising the cardholder card data.

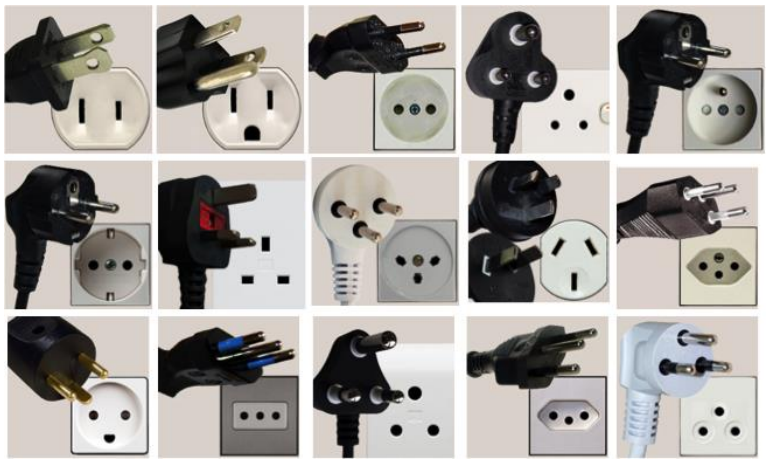
The IFSF protocols standardize communications with the payment terminal but not the physical attributes of the terminals. Following feedback from the manufacturers of on-street payment equipment the work group decided that it was important to include standards for certain physical attributes within IPIPS. EPA has negotiated an agreement with the European Vending Association to utilise certain of their standards for this purpose.

7 Why a standard?

Let's consider two different situations:

With batteries there are international norms. These allow appliance manufacturers to design their products using a type of standard battery. They also allow different battery manufacturers to produce batteries of any type providing they are compliant with the type definition. What if there were no standards for batteries?

.



On the other hand, there is NO international standard for electricity. Plugs, voltage and frequency differ from country to country. Nationalism protection which brings higher costs and a headache for international travellers and for manufacturers who sell into the different national markets.

7.1 What the adoption of IPIPS will do for the parking industry

From the examples above and many others such as smart phone charging devices it is clear that standards facilitate interoperability and transparency as well as reducing costs. For the parking industry adopting IPIPS payment standards will*:*

- Give operators confidence to define their investment strategy with a clear roadmap
- Enable suppliers and service providers to offer standardized equipment and services across Europe
- Allow international operators to create a single European wide compatible operation
- Help free all operators from country specific regulations and allow local operators to benefit from international working standards and economies of scale.
- Enable operators to accept electronic payments from foreign customers without any additional effort

- Reduce costs (investment, installation, maintenance and evolution through easier and simpler updates of the software used by the payment systems.)
- Lower on-going costs – reduced maintenance, less breakdowns, less expensive equipment upgrades, easier upgrades especially in payment software. A minimum of 10 years availability of components (IFSF mandate) will guarantee continuing availability of the solution
- Allow simple "card-in/card-out" operation to be widely used in car parks
- Streamlined procurement processes with specifications and selection criteria based on established standards.
- Stimulate the development of new IPIPS compliant payment applications with the potential to increase revenues.

Lastly, and perhaps most importantly, the adoption of IPIPS standards will demonstrate to the other very powerful players in the card payment ecosphere (banks, schemes, etc.) that the Parking Industry is capable of coordinating its efforts and speaking with **one** voice to protect the interest of all of the operators. Through the EPA's work on IPIPS, Visa Europe has recognised that EPA is the best organisation for it to communicate with the European parking industry. As this recognition grows and spreads to other organisations such as the European Payment Council (where the EPA is represented) EPA will gain much greater weight in discussions in the future.

7.2 What is the scale of the financial benefits that standards can bring?

It is extremely difficult to accurately measure the financial benefits that the widespread adoption of a standard will bring. It is however possible to identify the areas where those benefits will be generated and in some cases to indicate the large scale of those benefits:

Operating savings

Even after the reduction of interchange fees there is still scope for significant savings. Standardization will provide economies of scale. As noted in Part 1, EPA estimated the combined turnover of the parking operations in Europe to be circa €26 billion. Assuming that 50% of that turnover is via card payments and that the average commission is 2% leads to a total commission cost of €264m. Every 0.1% reduction in the commission creates €13.2m of savings for the industry.

Depreciation savings

IFSF mandates a minimum of 10 years availability of components. Adopting IPIPS will extend the operational lifetime of equipment from 8 to 10 years. Thus reducing the annual depreciation by 20%

Equipment savings

The adoption of IPIPS will ensure interoperability. This will lead to savings for the parking equipment suppliers. It will also reduce the cost of certification of their products in the different national markets.

Innovative developments

Last but not least, as noted above the adopting IPIPS will stimulate the development of new IPIPS compliant payment applications with the potential to increase revenues. It will also allow operators to focus on their strategy in payments selecting the most "future" proof solution instead of being led by payment solution providers.

8.1 Adopt IPIPS standards

The work group plans to publish the IPIPS standards before the end of 2015.

EPA will finalise the business model for the maintenance of IPIPS before the end of the year. The success of the E-payment initiative requires a strategic long term commitment from EPA to support its members and help them face the major challenges that new technologies and societal changes are bringing to the parking industry.

8.2 Build on IPIPS

The EPA e-payment initiative has the potential to transform EPA by providing a service that will benefit the parking operators both private and public as well as providing some advantages for the equipment suppliers.

Through the e-payments initiative EPA is serving the parking industry by providing guidance to its members and facilitating the sharing of resources for the benefit of all. The parking industry is a fragmented industry with a few large and many small and medium sized operators and suppliers. The parking operators individually are too small to create any pressure in the payment industry. The EPA initiative is bringing the industry together and giving it a voice in discussions with the payment industry. Working under the umbrella of the petrol retail industry strengthens that voice.

IPIPS is only the first step on a path that hopefully will lead the parking industry to understand the benefits of sharing certain resources that are non-competitive. Examples of this approach can be seen in the banking industry with a system like SWIFT, in the SEPA environment with the IBAN or the consortium of US merchants behind the Merchant Customer Exchange (MCX). It can be seen also in the aviation business where reservations systems are shared between airlines (for example NAVITAIR). It can be seen in car manufacturing where even competing manufacturers (Ford & Peugeot) share the same engine.

The parking industry must learn from these examples and become more effective in sharing resources and developing solutions. With the increasing pace of developments in technology there are a number of significant changes on the horizon that will create challenges for those who own and operate car parks. Some “experts” are even predicting the end of the parking industry as cars become driverless. Cars will either take themselves home between trips or cruise the streets until they are required again. Others say that “intelligent” cars will direct their drivers to the cheapest parking near their destination. Already, many car park operators are finding themselves tempted or forced to share their income with emerging businesses who promote ‘new ways to pay’ for services.

Without a co-ordinated international response, other interested parties (such as the car manufacturers and the payments industry) will use the new technologies in ways that will challenge the profitability of parking operators. EPA and the national associations must work together and sponsor initiatives that enable our members to work together to meet the challenges facing our industry.

The IPIPS concept is realistic and practical, more time, efforts and (financial) resources will be required to develop the Operating Guide and ensure that the benefits of IPIPS can be fully realised. If operators adopt them and specify IPIPS in their tenders for parking equipment, the European operators can take control of their payment (investment) strategy based on their own specific requirements and negotiate the best deals in a liberalised market.

8.3 What does the future hold

Adopting IPIPS standards will help the parking industry to anticipate trends and plan accordingly.

...in the next 5 years?

We can anticipate to observe

- Dilution of the card schemes and banks' dominance – acquirers as we know them will disappear and bank dominance will be diluted by new national and regional schemes.
- New entrants joining the schemes – such as government operations and new banks (e.g. Virgin Bank)
- Real time settlement of funds
- The borders between offline and online payment worlds will diminish (due to innovations like using a phone as a bank card)

Also, parking will be more connected to other markets and become less isolated (parking is never a goal in itself but a means to go somewhere)

...in the next 10 years?

We can anticipate the appearance of

• New card schemes

• Retailers becoming banks (but more commercially aware) such as the MCX initiative in the US (see Interchange fees above).

...in the next 15 years?

No one knows for sure … however the IPIPS standards will continue to protect the operators and allow them to invest wisely.

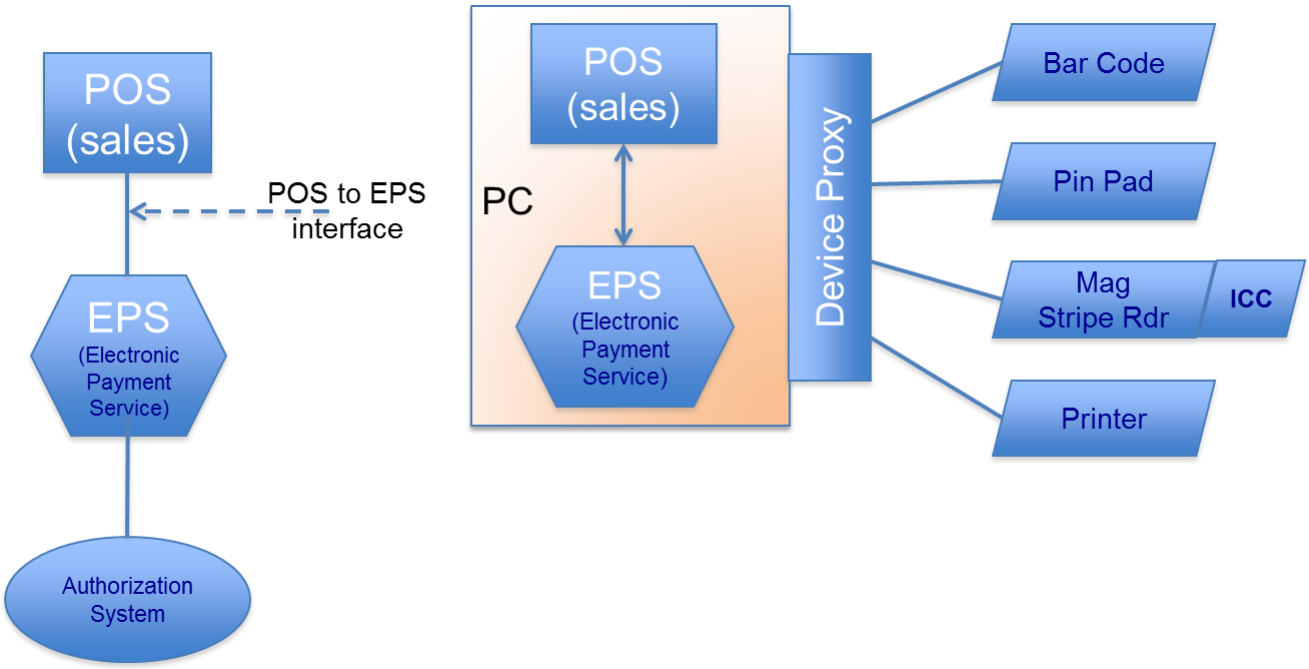
Part 3 Appendices

The IPIPS (powered by IFSF) standard consists of a few key elements:

9.1 POS to EPS

Point of Sale to Electronic Payment Server

The diagram below illustrates the logic behind the first layer of the payment process, isolating the payment terminal from the POS (Paystation) and therefore relieving the parking infrastructure from PCI compliance (and costs).



This POS-to-EPS standard is the cornerstone of the whole standardization process.

By having PMS suppliers incorporate payment terminals that comply with the IPIPS POS to EPS standard they will reduce their development and certification costs. One consequence is that it will help operators in swapping their terminals based on the best service they can get.

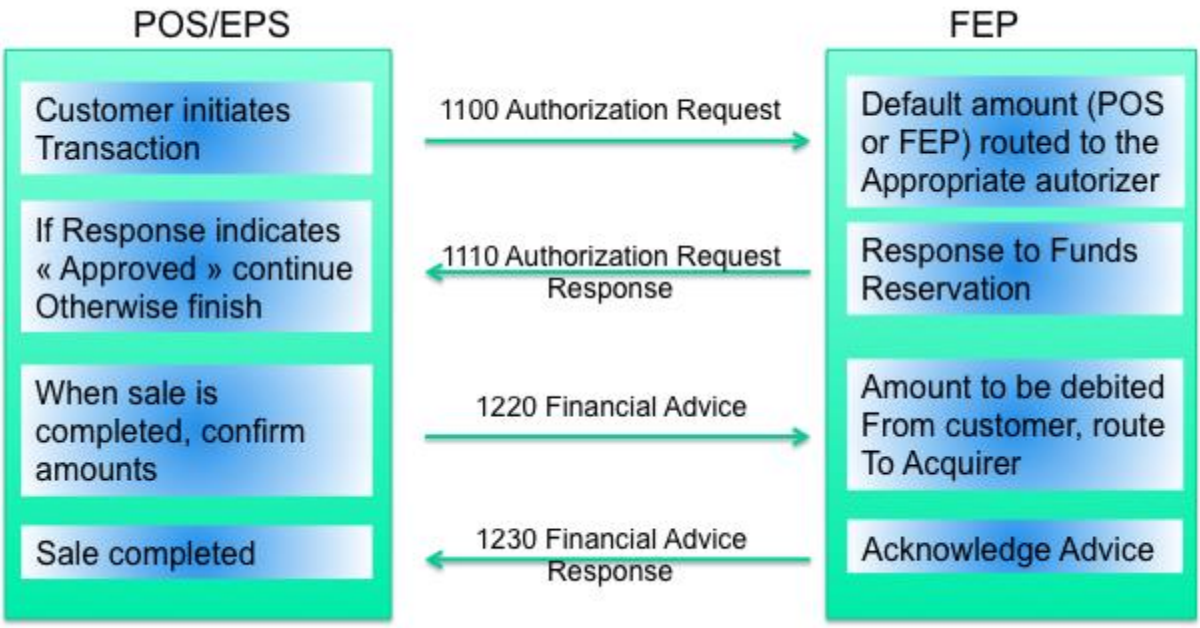
Obviously PMS vendors may be reluctant to relinquish the control they had on operators but in the end it will be a “win-win” situation.

9.2 POS to FEP

POS (Payment Terminal) to Front End Processor

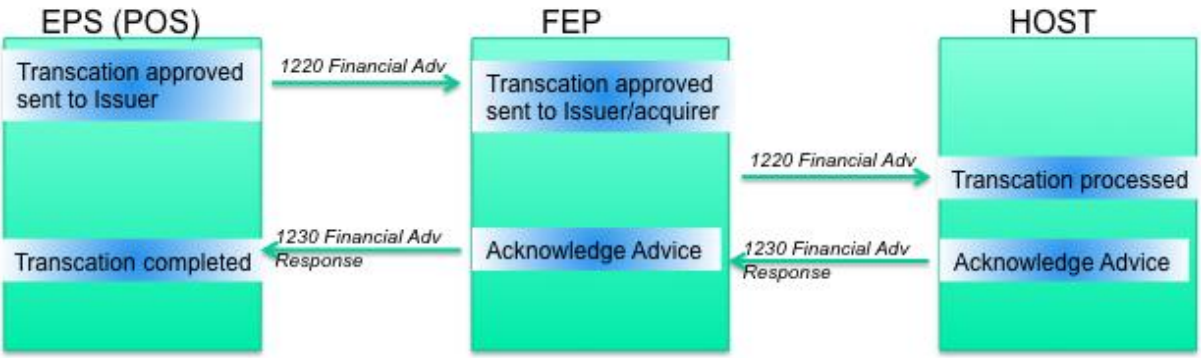
FEP or Front-End Processor is the gateway to the authorization system

This second standard deals with the transmission protocol from the EPS to the authorization server (whether PSP or Bank)



9.3 HOST to HOST

The last layer of the IPIPS standard concerns the transmission of the payment transactions from the FEP to any host whether the acquiring bank or the operator's own IT infrastructure.



9.4 SECURITY

The above layers are compliant with EMV and PCI requirements and the key management needed to encrypt the payment data.

9.5 Mobile Payments / Mobile Wallet

As mobile payments rapidly become more mainstream, the complexity of managing and processing transactions via multiple channels remains a continuous issue, influencing user experience (UX) and therefore the adoption of new payment methods.

The current lack of unification in the mobile payments market stems directly from the large number of competing technologies and differing mobile strategies.

Mobile wallets, integration with cards, online and now in-store mobile payments leave a range of options; none of which are available across channels.

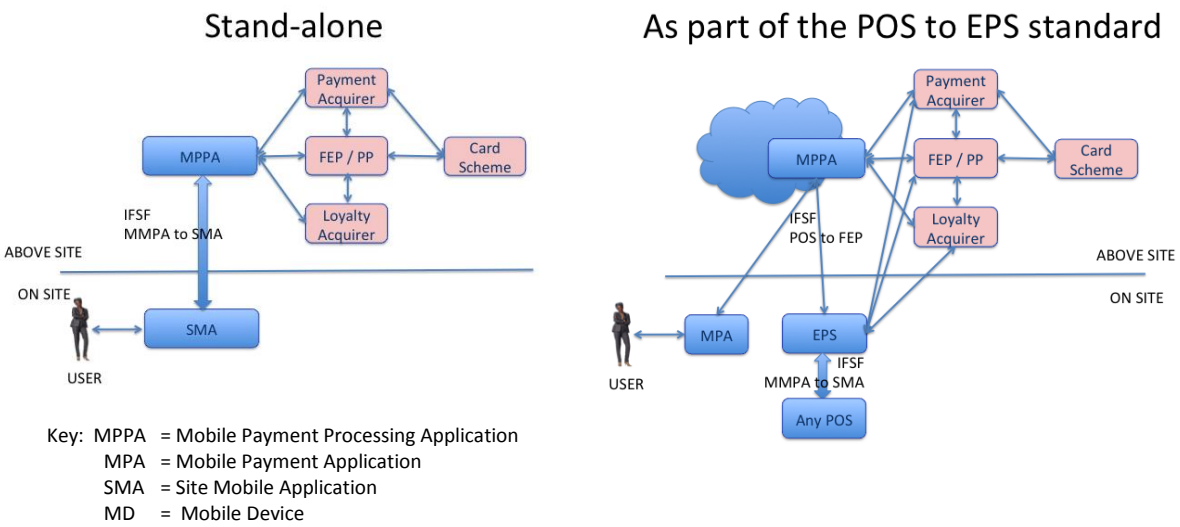
In addition to the classic brands like Mastercard and Visa, mobile wallets provided by others (such as Google) are becoming available

In most cases, the UX is too complicated. Without a standardized protocol for payment acceptance, mobile payments remain a complex process. Users are unable to use them as a consistent method to pay due to the difficulties of understanding, managing and maintaining them.

Security is also a key element which is sometimes overlooked by the mobile payment application providers.

The work done by EPA in conjunction with the IFSF EFT group has resulted in defining a mobile payment standard which is independent of all parties involved in the mobile domain (see Figure 12). It focuses on the format required by the Unsolicited Message originating from the MPA to the PSP.

The standard can operate in two different environments, either as a standalone payment method or in conjunction with the payment terminal:



Key: MPPA = Mobile Payment Processing Application
MPA = Mobile Payment Application
SMA = Site Mobile Application
MD = Mobile Device

Figure 12 Proposed Mobile Standards

10 Glossary

ACRONYM	DEFINITION
A/C	Bank Account
AAC	**A**pplication **A**uthentication **C**ryptogram.
AC	Application Cryptogram.
ALPR	Automatic Licence Plate Recognition. Method to automatically identify the vehicle through its vehicle licence (number) plate using optical character recognition.
AMEX	American Express
ANSI	**A**merican **N**ational **S**tandards **I**nstitute.
AR	Receipt Acknowledgement
ARPC	Authorisation Request Response Cryptogram.
ARPC	Authorisation Response Cryptogram
ARQC	Authorisation Request Cryptogram.
ATM	**A**utomated **T**eller **M**achine
BIN	**B**ank **I**dentification **N**umber. First part of PAN identifies type of card and issuing bank or other organisation.
Blocklist	List of all stopped card numbers (of a particular card type). Transactions should not be allowed on these cards and liability for losses accepted on blocked cards lies with the merchant.
BNA	Bank Note Acceptor. A machine that accepts notes as payment.
CB	Cartes Bancaires
CNIL	French National authority re- IT and freedom
CT	**Credit Transfer** – an irrevocable payment transaction initiated by the payer which results in transferring an amount of money from a payer's account to a payee's account.
Cutover	Day end closure. The process whereby a POS terminal closes the current batch and opens a new one, usually related to a Reconciliation transaction.
CVC	**C**ard **V**erification **C**ode
CVM	**C**ardholder **V**erification Method.
CVV	Code Verification Value
DCC	Dynamic Currency Conversion.
DD	**Direct Debit** - A direct debit or direct withdrawal is a financial transaction in which one person (company) withdraws funds from another person's bank account.
DDA	Dynamic Data Authentication
DES	Data Encryption Standard. An algorithm or encryption method commonly used for creating, encrypting, decrypting and verifying card PIN data. Depends on secret keys for security. Increased key length increases security. Normally 64 bits, of which 56 are effective.

DUKPT	Derived Unique Key Per Transaction. Encryption method where the secret key used changes with each transaction. More secure method than the predecessor, zone keys.
EA	Authentication Element
EFT	Electronic Funds Transfer. Card transaction or plastic money. Also includes loyalty card transaction.
EMI	E-Money Issuers
EMV	Europay, Mastercard, Visa. Organisation formed by 3 members to promote new standards for ICC.
EPS	Electronic Payments Server – a hardware and software application integrated with the site systems that processes payments (mobile or conventional) with an off-site payments application.
EU	European Union
FEP	Front End Processor. A computer used to respond to card authorisation requests and capture card sales data. Implies an Esso controlled computer unless qualified in some way. Eg: Bank FEP or Loyalty FEP.
GSM	Global Systems for Mobile Communication
HSM	Hardware Security Module. A tamper-proof box that may be attached to the FEP or part of a PIN pad. Contains secret keys used for PIN verification, encryption, MAC'ing and other security related purposes.
IC	Integrated Circuit
ICA	Interbank Code Association - 4 digits identification number through which each member of MasterCard International network is referred to.
ICC	Integrated Circuit Cards. Chip or Smart cards containing a microprocessor.
ID	Identifier
IEA	Indoor Exception Authorisations.
IFD	Interface Device.
IP	Internet Protocol
IPT	Indoor Payment Terminal – a device installed at POS lane with consumer input capabilities (e.g. PIN entry)
ISDN	Integrated Services Digital Network
ISO	International Standards Organisation.
ISO 20022	ISO 20022 - Universal financial industry message scheme (which used to be also called "UNIFI") is the international standard that defines the ISO platform for the development of financial message standards.
ISO-code	First part of PAN which identifies card type. International Standards Organisation (ISO) allocates codes to different organisations for their use. Eg: Esso Cards in Europe use 7033 or 7064, followed by a country code. See also BIN.
ISO8583	ISO standard for Financial transaction (card originated) interchange.
IT	Information Technology
JCB	Japanese International Card scheme

Key card	Method by which a loyalty customer uses another (payment) card as key to their loyalty account. LE maintains cross reference between numbers.
LE	Loyalty engine. This may be part of the FEP or a 3rd party system used to carry out loyalty functions.
LFEP	Loyalty Front End Processor – the application or institution the Site uses for the processing of loyalty rewards or loyalty transactions.
Luhn	Final (check) digit of PAN. Used to ensure PAN recorded correctly and detect false cards.
MAC	Message Authentication Code. A code generated from the message by use of a secret key, which is known to both sender and receiver. The code is appended to the message and checked by the receiver.
MAC	Authentication Message Code
MCC	Merchant Category Code
MCE	MasterCard Europe
MCI Network	MasterCard International Network
MD	**Mobile device** - the mobile device (e.g smart phone) used by the consumer to interface with the mobile payments application (MPA)
Merchant	Retailer who has card acceptance agreement with an acquirer (or sometimes directly with an issuer). If merchant follows card acceptance rules he is guaranteed settlement for the value of card transaction.
MNO	**Mobile Network Operator**- the infrastructure provided by a network operator to facilitate data and voice calls or WIFI
MOP	Method Of Payment at the POS. Cash, cheque, card, local account, voucher etc.
MPA	**Mobile Payments Application –** the application that the customer has subscribed to enable the payment of transactions using a MD.
MPP	**Mobile Payments Processor** - this is the supplier of the application that provides communication between the MPA, the site and the PP. They will provide an application (the MPPA) that enables the transactions to be processed and transactions to be enabled and settled.
MPPA	**Mobile Payments Processing Application** - the application provided by the MPP that provides communication with the MPA, the site and the PP to instruct the site to release dispensers, process transactions and obtains necessary authorisations and other data from the PP.
MTI	Mobile Transaction Identifier – Single use transaction identifier assigned by the MPPA.
On-us	Term that refers to Financial Transactions that are verified and authorized on the FEP. 'Not on-us' is used to denote transactions that are routed elsewhere for authorization.
OPT	**Outdoor Payment Terminal** - a device installed at a retail petroleum site to enable payment outdoors without direct intervention from a site operator. For the purposes of this document, this may be a single device mounted in a central position that controls multiple dispensers or a device integrated into each dispenser.

PAC	**Personal Authentication Code**. Method of ensuring key data on magnetic stripe of card not altered and may also be used as indirect method of verifying PIN, as for Esso Card Mark II.
PAD	Packed Assembler/Disassembler
PAN	Primary Account Number. Card number, usually 16 or 19 digits.
PC	Personal Computer
PFEP or FEP	**(Payment) Front End Processor**- (sometimes referred to as the Front End Processor or FEP) - the application or institution that the Site uses for the processing of payments. This may be a third party provided application made available as a service or an in-house application provided by the MPP or a major fuel brand.
PIN	**Personal Identification Numbe**r. Number linked (normally) to an individual card that is used to verify the correct identity of the user instead of signature verification. Depends on an algorithm such as DES using secret keys.
PIN pad	Numeric keypad for customer to input PIN. Normally integrated with HSM and often with card reader.
PKE	PAN Key Entry. Recording a card transaction by keying the embossed card details (PAN, expiry date, etc) into the POS to create an electronic transaction even for a card which cannot be swiped eg: because it is damaged.
PMS	**P**arking **M**anagement **S**ystem - a central controlling device installed at the site which enables communication of data and controls to all devices in a parking site
POS	Point of Sale - the device (hardware and software) that is used to process transactions on the site
Private fields.	Data fields in the ISO8583 specification for private use to be agreed between the sender and receiver of the message.
PVC	Polyvinyl Chloride
PVV	Algorithm name - based on a 3DES and implemented in B0' v3 in order to double the stripe PIN-coding key length
R&D	Research & Development
RFID	Radio Frequency Identification. A radio transponder that identifies the customer or vehicle at a site. Also used to identify EMV contactless devices.
RFU	Reserved for Future Use. The makeup of any field to be used for future use will be allocated at the time of use.
RN	Retail Network - the infrastructure provided by or to the site operator to enable transaction and other data to be shared between the site and other services off-site (e.g. for payment processing and loyalty processing).
RP	Remote Payment
RSA	Rivest, Shamir, Aldeman
RTC	Phone current network
SAM	Secure Authentication Module
SDA	Static Data Authentication
Site	Parking site

Site System	Site System Components including, but not limited to, POS, EPS, site controller. Also refered to as PMS (Parking Management System)
SSL	Secure Socket Layer
SVC	Stored Value Card
T&E	Travel & Entertainment
TC	Transaction Code
TCP/IP	Transmission Control Protocol/Internet Protocol. A telecomms protocol (standard) for transmission of data between two computers.
TD	Ticket dispenser : mechanism that delivers a ticket at a parking meter or entry/exit barrier
Tokenization	**Tokenization** is the process of substituting a sensitive data element with a reversible benign substitute. In the payment card industry, tokenization is one means of protecting sensitive cardholder personally identifiable information in order to comply with industry standards and government regulations.
TP	Transaction processing
Track 2	One of 4 (0, 1, 2, 3) tracks on magnetic stripe of a card. Most commonly used track is Track 2, which contains 37 characters.
Track 3	One of 4 (0, 1, 2, 3) tracks on magnetic stripe of a card. Track 3 is relatively uncommon and mostly used for Bank Debit /ATM cards in some countries like Norway and Germany (or to carry extra customer information to print on receipt). Contains 107 digits.
Triple DES	Significantly more secure implementation of DES algorithm and becoming an increasingly common bank requirement. Plaintext is enciphered, deciphered and re-enciphered using 3 different keys.
TVR	Terminal Verification Results.
UM	**Unsolicited Message** from the cloud (or another source) to the site initiated by a MD.
VA	Authentication Value
VE	Electronic Value
VISANET	Visa clearing format
VS	Static authentication Value
Wallet	Wallet. Place where card data &/or credentials are securely kept
X25	Communication Network for French Interbank Network (old technology of "Packet switching")