Document EPC492-09
Version 2.0
Date 18th June 2010

WHITE PAPER
MOBILE PAYMENTS
1st edition

European Payments Council

Table of Contents

Executive Summary

The role of the EPC is to ensure the evolution of an integrated market for payments in Europe through the development and promotion of standards, best practices and schemes.

Mobile phones have achieved full market penetration and rich service levels in most, if not all, Member States, making the mobile channel ideal for leveraging and promoting the use of SEPA (Single Euro Payments Area) instruments.

This "white paper" endeavours to:

- Inform stakeholders of EPC's commitment to mobile payments in SEPA;
- Provide business rationale for entering the mobile payment services market;
- Demonstrate the customer adoption potential of mobile payments by presenting several realistic and illustrative scenarios for the use of mobile payments;
- Outline the prioritised categories for mobile payments;
- Specifically analyse mobile contactless SEPA card payments;
- Collect stakeholder views and feedback.

The white paper has been written in a non-technical style to inform payment service providers, their customers and all the stakeholders involved in the payments value-chain about the EPC's initiative for mobile payments in SEPA.

The first sections provide a high-level business rationale for entering the mobile payment services market, an introduction to mobile payments in relation to SEPA instruments and a risk management foundation justifying the key role of the "secure element". Next, through examples of "use cases" facilitating the daily life of a hypothetical customer, it is shown how mobile payments can ensure efficiency, effectiveness and convenience. This is followed by the introduction of a general-purpose classification approach for the different mobile payment types, including mobile contactless and mobile remote payments. To further highlight the feasibility and advantages of mobile payments, several fully-illustrated sections are devoted to the introduction of extra detail for some significant mobile payment categories, as well as illustrating some approaches for subscription to mobile services.

Thereafter the mobile contactless SEPA card payment category is explored in more detail. This is done by addressing several business aspects, including how mobile payments do not modify the roles of existing stakeholders during the actual card payment transactions, and how service provisioning can be accomplished in coordination with the new players introduced by the mobile services ecosystem. The document further presents a high-level analysis of important considerations such as mobile-specific technologies including specific choices for the secure element, the user experience through the mobile phone interface, the point-of-sale infrastructure and, finally, mobile standardisation and industry bodies.

Finally, a dedicated annex provides a generic analysis of all types of available secure element technologies.

A second edition of this document is scheduled for Q1, 2011. According to the prioritisation established by EPC, it will include a more detailed analysis for mobile remote payments.

This document is self-contained. For interested readers requiring more detail, EPC will provide further implementation guidance on mobile payments in forthcoming documents for both contactless and remote payments covering business, technical, security and legal aspects.

1 General

1.1 About EPC

The EPC develops the payment schemes and frameworks necessary to realise the Single Euro Payments Area (SEPA). SEPA is an EU integration initiative in the area of payments designed to achieve the completion of the EU internal market and monetary union.

SEPA is the area where citizens, companies and other economic participants can make and receive payments in euro, within Europe, whether between or within national boundaries under the same basic conditions, rights and obligations, regardless of their location.

Figure 1: SEPA coverage

EPC defines common positions for core payment services (known as SEPA payment instruments) within a competitive market place, provides strategic guidance for standardisation, formulates best practices and supports and monitors implementation of decisions taken. This is done in such a way that banks can maintain self-regulation and meet regulators' and stakeholders' expectations as efficiently as possible.

EPC now consists of more than 70 members, composed of banks and banking associations. Over 300 professionals from 32 countries and representing all sizes and sectors of credit institutions within the European market are directly engaged in the work programme of the EPC.

A more detailed introduction to SEPA payment instruments can be found in Annex IV – SEPA Payment Instruments.

1.2 Vision

The vision of EPC is to ensure the evolution of an integrated market for payments through the development and promotion of standards, best practices, and schemes. The further dematerialisation of payment instruments which could ensue would contribute to foster economic growth in SEPA.

Following this line, the EPC has been chartered by its member banks and payment institutions to leverage their existing leadership position for the practical deployment of mobile payments in SEPA.

The payment transactions enabled by mobile devices and services should build on existing SEPA Rulebooks and SEPA Cards Framework and (global) standards as far as possible. Therefore, EPC specifies rules, standards and guidelines to create the necessary environment so that payment service providers can deliver secure, efficient and user-friendly mobile solutions to access the SEPA payment instruments.

Cross-industry cooperation, especially between the banking sector and mobile network operators (MNOs), has been identified as a critical success factor. Hence EPC commits itself to help facilitate cross-industry cooperation on rules, standards and best practices in this area. Customers (see Annex I - Definitions) should not be bound to a specific mobile network operator or a particular handset and should retain their current ability to switch between payment service providers.

1.3 Scope and Objectives of this Document

The purpose of this white paper is to present an overview on mobile payments for SEPA. This means the usage of the mobile channel for the initiation of SEPA payment instruments. Although the first edition of this document includes both contactless and remote payments, only contactless card payments are elaborated in more detail according to the priorities set by EPC (see section 3.2.2). A second edition of this document is scheduled for Q1, 2011 and will include a more detailed analysis for mobile remote payments.

This white paper is structured as follows:

- Chapter 1 provides general information about EPC and its vision;
- Chapter 2 is an introduction to SEPA, mobile payment services and related business rationale;
- Chapter 3 portrays a number of mobile payments which are introduced via several user-centric usage scenarios. It further contains the categorisation of the mobile payments by EPC and a high-level description with diagrams of the use cases as well as some subscription processes;
- Chapter 4 treats a number of business and technical aspects for mobile contactless card payments in more detail;
- Annexes with definitions, abbreviations, bibliography and an introduction to SEPA payment instruments, and a dedicated annex on secure elements is included which provides a generic analysis of all types of available technologies.

With the publication of this white paper, EPC has the following objectives:

- Inform stakeholders about EPC's commitment to mobile payments in SEPA and the potential of the mobile channel to leverage SEPA payment instruments;
- Inform on the new convenient, homogenous and seamless services access and new business opportunities enabled by the mobile channel;
- Outline the prioritised categories for mobile payments;
- Specifically analyse mobile contactless card payments;
- Provide other information and examples of existing mobile payment deployments.

1.4 Out of Scope and Future Documents

This document is intended to be self-contained. It shall be noted that it is not meant to be an exhaustive introduction to all aspects of mobile payment services but rather focuses on the initiation of payments via the mobile channel leveraging existing SEPA payment instruments (SCT, SDD and SEPA for Card Payments). The reader is referred to EPC standards and rulebooks (www.europeanpaymentscouncil.org) for the general aspects of the transaction leg in mobile payments.

The document does not contain market research since numerous studies are already available.

Although this document describes some elements for the business rationale for payment service providers wishing to enter the mobile payments market, more details will be provided in forthcoming "Mobile Payments Implementation Guidelines" to be issued by EPC. These guidelines will also further elaborate on technical aspects, such as mobile wallet design guidelines, and security aspects, such as the risk associated with the usage of the mobile phone, "personal codes" and PIN procedures.

1.5 Audience

The document is primarily intended for the following stakeholders:

- Payment Service Providers (Banks and Payment Institutions) and Card Schemes;
- Customers (Payers, Payees and Cardholders);
- Merchants and Merchant Organisations.

In addition, the document may also provide valuable information to other parties involved in implementations and deployment of mobile payments, such as:

- Mobile Network Operators (MNOs);
- Trusted Service Managers (TSMs);
- Equipment Manufacturers;
- Application Developers;
- Public Administrations;
- Regulators;
- Standardisation and Industry Bodies.

2 Introduction

2.1 Evolution of Mobile-Based Services in SEPA

Consumers expect that new technology will continue to facilitate the convenience of carrying out daily and repetitive tasks. For example, an area that is still generating a great deal of attention is the necessity to use hard cash in conducting many commercial and personal daily payments. It is now widely accepted that some pervasive new technology-based solution should be introduced to minimise this problem.

Also, consumers demand that whatever the ultimate nature of new technologies, processes or products, they should not add any significant shortcoming to the existing solutions they are supposed to improve upon. Furthermore, although there are already some service offerings capable of substituting cash, so far no technology or product has achieved the necessary acceptance to become a true alternative, chiefly because new burdens were added that consumers were not ready to accept.

According to [10] the current penetration of mobile phones in the developed economies is 97%. Many consumers are already using mobile phones for services beyond the traditional voice calls and short messaging services (SMS). These services have been greatly facilitated by the current MNO infrastructure supporting packet-oriented Internet access through GPRS and 3G technologies through virtually full geographic network coverage. Recently, consumer expectations for mobile phone functionality have increased dramatically. This is signalled by the fact that the "Smart Phones" market segment is growing more strongly, and at a much higher rate than any other segment [7]. Consumers are assuming this trend will continue and are eager to embrace new service solutions based on this delivery platform. Clearly financial services are recognised as most important among these new mobile services, hereby setting high expectations. EPC, together with many other financial organisations and institutions, believes that mobile-phone initiated payments will be very well received.

Merchants demand that new technology solutions provide a direct improvement to the efficiency of their operations, ultimately resulting in cost savings and in an increase in business volume. Merchants also expect that new technology reduces exposure to security issues (such as cash theft) and liability (such as illicit payments). Finally, merchants expect that new service offerings introduce new opportunities for marketing and increased brand strength. EPC believes that mobile-phone based payments, in particular those using the contactless approach, are very well positioned to achieve all these benefits for merchants and other stakeholders who are directly providing services to consumers.

In relation to the personal consumer space, the availability of practical SEPA person-to-person mobile payments, either account or card based, would provide additional means for further cash and cheque displacement.

Finally, according to [1] many payment service providers have already identified mobile payments as their target for their new growth opportunities. Different mobile payment pilots and commercial deployments are conducted in SEPA and elsewhere, where stakeholder feedback has been consistently very positive. Therefore the SEPA marketplace is clearly set for an immediate uptake of mobile payment services.

2.2 Business Rationale for Entering the Mobile Payments Market

By definition the ecosystem for mobile payments, whatever form it may take, will provide in its value-chain for a role for payment service providers that hold customer accounts (Banks, Payment Institutions or e-money institutions). Although this white paper is not intended to build a business case for payments institutions in mobile payments (since this lies in the competitive space, see section 2.4) it aims to demonstrate that there exists, in 2010, a powerful business rationale to do so.

One of the objectives of the EPC, as expressed in its vision and roadmap, is to stimulate the development and implementation of mobile payments within banks and ensure that member financial institutions play a prominent role in the mobile payments value chain.

As previously stated, the document does not include any market data and research. The reader is invited to read through the numerous market studies available, which show that, besides strong market potential, mobile payments are already taking up. They also predict rapid growth rates in the use of mobile phones for financial transactions.

Each payment service provider should determine individually if, ultimately, it has a business case based on market research, potential revenues and estimated investments and costs. It should further define its position, the resources it is prepared to invest and the role it wants to play in the value-chain. The business case will differ for each provider depending on its customer base, business strategy and objectives, geographical environment, technical infrastructure, available resources and expertise.

The major elements supporting a business rationale are the following:

- strong penetration of mobile phones: in the last couple of decades the number of mobile phones has by far exceeded the number of payment cards worldwide, and more and more customers are ready and willing to use the mobile channel for payments;
- leverage the recent SEPA payment schemes and framework investments by adding mobile phone initiated payments to its service offering;
- provide user convenience by meeting proven needs by both customers and merchants (see Annex I - Definitions), thereby allowing customer retention and even expansion towards the new generation of mobile phone users;
- the need to foster innovation with competitive offerings in a more complex ecosystem including new players, in line with the EPC SEPA vision, thereby growing the market for payments and migrating customers to faster, more efficient and more convenient means of payment.

The strategy in which a payment service provider may enter the market, should it decide to do so, including the concrete business model and the interactions with other stakeholders in the value-chain, are not discussed in this white paper. However, various business models will be presented in the forthcoming "Mobile Payments Implementation Guidelines" documents wherein the EPC aims to further inform the payment service providers in their decision making process.

Clearly, the mobile phone will be an additional payment initiation channel, co-existing with other channels and means of payment. Other alternatives exist and the payments business is not limited to SEPA frontiers.

2.3 Security Aspects

Financial institutions have a strong reputation for settling payment transactions in a secure way. Merchants and customers are very sensitive about security. Therefore, the relationship between a payment service provider and its customers can be severely damaged if there is any doubt about security in payment transactions.

The acceptance of new payment services relies upon the trust the customers show to their payment service providers (with which they have a contractual relationship) and the transparency of all the underlying processes.

To maintain a similar trust and transparency towards customers for mobile payments as for existing payment initiation channels, it is fundamental to establish a secure, homogeneous ecosystem also encompassing the new participants where it can easily be understood that:

- responsibilities are assigned;
- security issues are governed;
- payment transactions are secured, comprehensible and reliable;
- privacy is respected;
- security management systems of the involved parties are consistent.

This all indicates that mobile payment service providers have to establish an overall security architecture that covers all security aspects of the mobile payments ecosystem following reputable international standards. This security architecture should cover at least the following aspects:

- Process Level

  Every service provider in the mobile payments ecosystem must ensure that an appropriate information security management system is in place. Each service provider must be able to either state this in a suitable way to auditors – preferable, because it is transparent to the customers – or to define it in terms of security service level agreements in the applicable contractual relationships.

  The information security management system contains at least methods and procedures to monitor and manage relevant risks, and assigns the appropriate resources and responsibilities to mitigate these risks. Every participating party has to define their responsibilities and the valuable assets to protect in their sphere of responsibility.

- Application Level

  For any use case there has to be a security concept documented. On this level the applications and work flows are known. The abstract components in terms of used devices, customer behaviour, attack surfaces, application environments, etc. can be described and used to analyse the threats and risks. This applies for the whole supply chain and can be broken down into the different perspectives of the customer, service providers, and contractual partners respectively.

- Implementation Level

At the implementation level, the choice of which security controls and measurements should be in place depends mainly on the technical solutions used to implement the services and the associated environment.

By analysing the specific implementation, the security attack surface can be identified and the appropriate countermeasures can be taken. The most salient countermeasure already identified is the "Secure Element", which is introduced in the next section.

On this architectural level it could be necessary to consider other security or regulatory requirements, as for example, the data security standard of the payment card industry (PCI-DSS).

The reader will find further details regarding security aspects in the upcoming documents to be issued by the EPC (section 1.4.).

2.3.1 The Secure Element as a Critical Component of the Mobile Payments Infrastructure

Similarly to plastic cards, enhanced security requires a so-called "Secure Element"(a formally-certified, tamper-resistant, stand-alone Integrated Circuit, i.e. a "chip") to store the customer's personal data, the issuer's payment credentials (security keys) and other critical data. In other words, the experience in card payments has shown that no other technology or business process is as efficient and cost effective as the chip in mitigating risk of fraud.

While the direction for plastic cards each featuring a dedicated Secure Element seems clear, we must now identify which feasible alternatives exist for the deployment the Secure Elements supporting Mobile Payments.

The main factors driving the choice of Secure Element for Mobile Payments are:

- intrinsic security properties and eligibility for formal certification;
- integration within the Mobile Phone and connections to external interfaces such as contactless or remote protocols;
- availability (timelines and geographical market);
- support infrastructure (personalisation tools);
- possibility of deployment within the existing commercial supply chains for Mobile Phones;

and

- total cost of ownership.

While it is possible that each mobile payment service provider deploys (directly or indirectly) its own secure element solution, it is clear that a well-coordinated selection of secure elements will provide significant advantages in:

- producing consistent and well-understood security properties nurturing customer trust;
- economies of scale by enabling a well-developed industrial supply chain and supporting infrastructure, including personalisation and certification;
- and reduced time-to-market for SEPA-wide deployments.

To provide further support in this subject, a dedicated annex has been introduced, (see Annex V – The Secure Element) providing extra rationale for the selection between the different alternatives.

2.4 Framework for Mobile Payment Services

The EPC is establishing high level principles and a framework for mobile payments in order to create the necessary standards and business rules for payment service providers in this new area. Mobile payments constitute a new channel to leverage existing SEPA instruments, i.e. the SEPA schemes (SCT, SDD) and SEPA Cards (SCP). The main focus is in the area of initiation and receipt of credit and debit payments (including card payments) through mobile phones. Mobile Payments will comply with the Payment Services Directive [14] as well as with the existing rules for underlying SEPA instruments. As a result, the mobile channel does not put any constraint on the value or type of payments generated through it (all SEPA instruments are transaction amount-neutral). This remains a competitive decision by each individual payment service provider.

The high level principles and a framework for mobile payments including (references to) standards rules and best practices developed by the EPC are made publicly available to market participants and providers within the mobile channel value chain. It will be the responsibility of each of them, or of any grouping thereof, to decide when and how to adopt these, and in particular towards which segment or segments of the payments market their products and services will be geared. This could be e.g., the micro-payment segment, or any other segment.

One of the strongest business opportunities of mobile payments lies in introducing omnipresent services replacing cash. These services should speed-up daily transactions and lower the general operational cost of business. EPC is particularly concerned with facilitating this by enabling highly-streamlined user experiences wherever risk management policies allow. In that respect EPC and other bodies are specifying minimum security requirements. However, the practical implementation of those remains in the competitive space.

EPC focuses on the areas that form the basis for interoperability, and not those lying in the competitive space. It will also foster cross-industry cooperation to enable the mobile handset to become an efficient channel to initiate payments.

The next figure illustrates the involvement of EPC in the different layers within the scope of mobile payments.

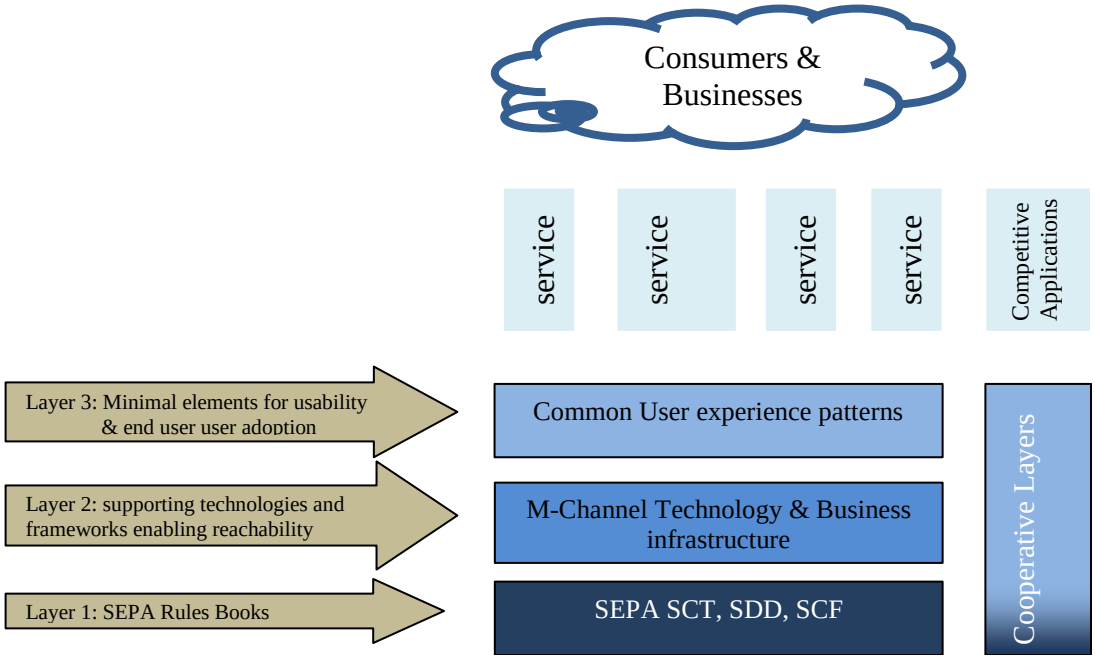

Figure 2: Scope of Mobile Payments. The gradient of blue denotes the level of cooperation in each layer.

Layer 1 denotes the already existing SEPA Rules Books for SEPA Credit Transfer and SEPA Direct Debit and the SEPA Cards Framework. This layer will not be altered for the specific use of mobile payments.

Layer 2 is defined as the supporting technologies and frameworks enabling reachability into the SEPA payment instruments. A notable example in this area can be found within the EPC document "EPC-GSMA Mobile Contactless Payments Service Management Roles - Requirements and Specifications" [18], which has been jointly developed by EPC and the GSM Association (GSMA)..

Layer 3 elements are, by default, mostly in the competitive space. But in order to overcome the potential complexity of the mobile phone user experience and to ensure reachability, minimal guidelines will be introduced. These guidelines will introduce behavioural patterns for a practical user experience and, when applicable, will define minimum security requirements to ensure the integrity of business chains to the benefits of users. Examples of areas completely left open for competition between different payment service providers are pricing, concrete user experiences, risk management, delegation with parental controls, reporting, co-marketing with merchants or other service providers, branding, etc..

3 Mobile Payments for SEPA

3.1 A Day in the Life of a Mobile Payments Customer

This section introduces how the daily life of a bank customer can be enhanced by using his mobile phone for payments (so-called mobile payments). A few examples are hereby presented to illustrate some use cases. It should be noted that many other variations and use cases exist for the deployment of mobile phone initiated payment services.

Mr. Garcia is a bank customer and a regular mobile phone user with a very busy life. Mr. Garcia particularly enjoys using his mobile phone beyond just phone calls and texting. The availability and convenience of this handy device at any time is compelling him to employ it for new types of services. In particular, the security and the control he has on it, creates for him an environment that he can trust to conduct payments. Figure 3 depicts a typical day in the life of Mr. Garcia.

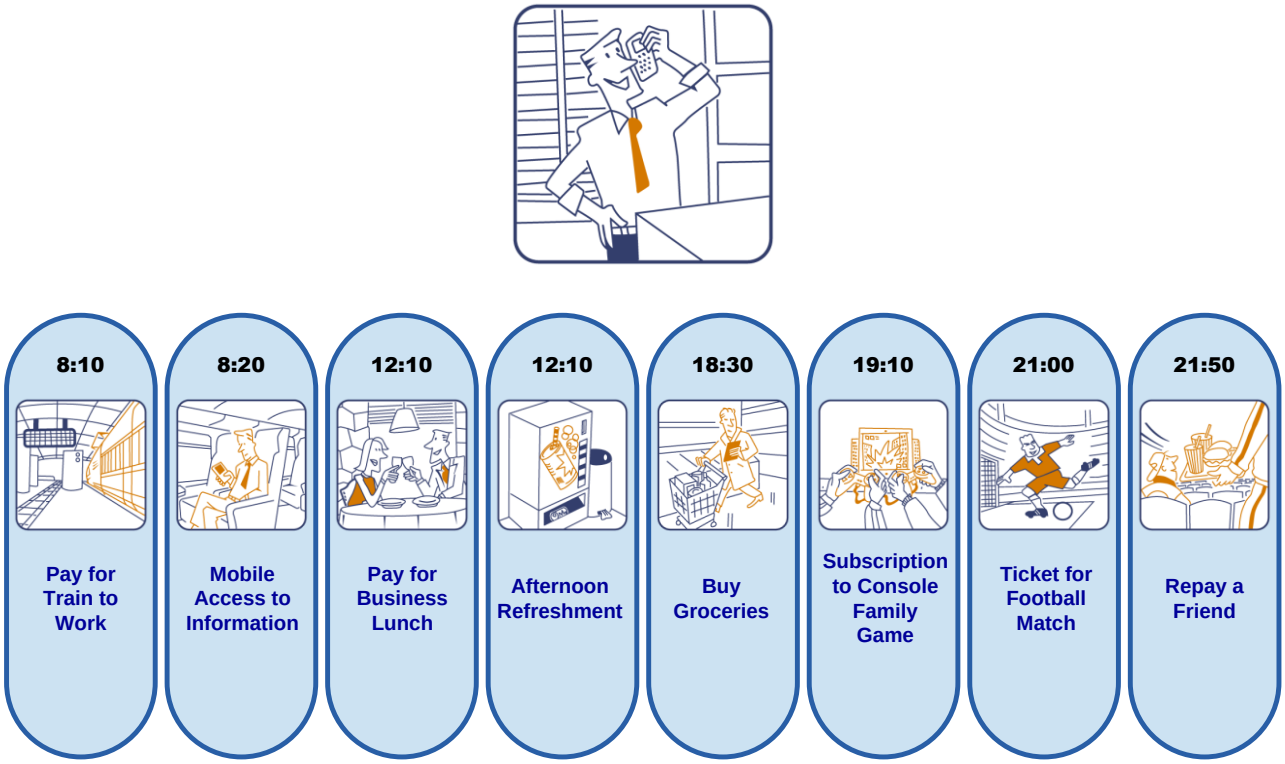

Figure 3: A day in the life of Mr. Garcia.

3.1.1 Pay for Train to Work

Mr. Garcia arrives at 8:10 at the train station to go to his office. When he reaches the entry gate to get to the platform, he tries to validate his monthly ticket by tapping his mobile phone by the gate's sensor. Unfortunately, he is informed that his ticket has expired. A specific message on his mobile phone display suggests he purchases a renewal. Mr. Garcia then decides to step out of the queue and purchase the renewal using his bank current account from the ticketing machine. He does that by directly confirming this on the mobile phone and subsequently tapping the ticketing machine with the mobile phone to make the payment transaction. Immediately the ticket renewal is obtained. Back at the gate he is now allowed access to the train platform. Thanks to this speedy process he makes it to his usual 8:15 train with ease.

3.1.2 Mobile Access to Premium Entertainment

Once comfortably seated in the train, Mr. Garcia decides to use his mobile phone to entertain himself on the journey. With his mobile phone he browses a video on-demand web site. However, the web site informs him that this is a paying service. Through a simple menu option on his mobile phone display, Mr. Garcia selects his credit card, details of which are embedded in the phone, to pay the web site. He subsequently obtains access to the requested movie.

3.1.3 Pay for Business Lunch

At lunch time Mr. Garcia invites a prospective customer. After checking the restaurant bill, he decides to use the embedded corporate card in his mobile phone to pay. This is achieved by selecting the appropriate card from the menu option on his mobile phone display, enabling it for the next transaction by entering his personal code and simply tapping his phone by the waiter's POS terminal.

3.1.4 Afternoon refreshment

By mid-afternoon, Mr. Garcia takes a short break for some energy recharging. Just outside his office there is a small food parlour with several vending machines. After making the selection for his preferred soda, he swiftly taps the payment terminal with his mobile phone to perform the payment with his regular current account. During this process, the vending machine recognises that a mobile phone has been used for the payment and instructs it to show Mr. Garcia the web-site of the soda brand for a special offer.

3.1.5 Buy Groceries

On his way back home, Mr. Garcia decides to stop by the local supermarket to get a few groceries. At the cashier he decides to use an embedded debit card in his mobile phone to pay. This is achieved by selecting the appropriate bank card from the options menu on his mobile phone's display. He then taps the cashier's POS terminal a first time with his mobile phone to obtain the payment details and enters in the mobile phone's keyboard his personal code. Finally he taps again the POS terminal with mobile phone to confirm the payment. Once paid, the terminal simultaneously updates Mr. Garcia loyalty card in his mobile phone with the points obtained from the new purchase.

3.1.6 Remote Subscription to Online Family Game

While browsing the Internet with the family's game console, Mr. Garcia's daughter finds a new subscription-based multiplayer game she likes to buy. To pay for it, Mr. Garcia enters his mobile phone number on the console screen. Immediately afterwards, the mobile phone displays the request for direct debit authorisation. By selecting this, Mr. Garcia authorises his current account as the target of the charges. His daughter can then start playing right away while Mr. Garcia leaves for the football match.

3.1.7 Ticket for Football Match

Tonight Mr. Garcia is meeting his friends at the stadium to support the local football team. At the stadium entrance, Mr. Garcia pays again with his mobile phone. He first selects the appropriate card from the menu option on his mobile phone display. Then he taps his mobile phone by the ticketing terminal, which updates the mobile phone with the football ticket. Afterwards, he enters the stadium by tapping his mobile phone by the entry gate.

3.1.8 Repay a Friend

At half-time break, one of Mr. Garcia's friends offers to get fish and chips. Upon her return, Mr. Garcia insists on reimbursing his friend. In order to do so, he first selects his friend's mobile number from his mobile phone's contact list. Then, by selecting his appropriate current account from the menu option on his mobile phone display, Mr. Garcia transfers the amount due to his friend's account. Finally his friend receives a message on her mobile phone display confirming the receipt of the credit transfer.

3.2 General Overview of Mobile Payments

3.2.1 Introduction

As mentioned in section 2.2, "mobile payments" constitutes a new channel to leverage existing SEPA instruments.

Mobile payments are broadly classified as "contactless" (also known as "proximity") or "remote" payments. For "contactless payments" the payer and payee (and/or his/her equipment) are in the same location and communicate directly with each other using contactless radio technologies, such as NFC (RFID), Bluetooth or infrared for data transfer. For "remote payments" the transaction is conducted over telecommunication networks such as GSM or Internet, and can be made independently of the payer's location (and/or his/her equipment). To leverage as much as possible the shared infrastructure for contactless SEPA card payments, mobile contactless payments are based only on the usage of near field communications (NFC) technology in card-emulation mode.

Depending on the nature of the payer and payee being a consumer[1] (person) or otherwise (business), mobile payments may be also classified as Person-to-Person (P2P), Person-to-Business (P2B), Business-to-Person (B2P) and Business-to-Business (B2B) payments.

The following table illustrates how the use cases described in section 3.1 can be implemented using the existing SEPA instruments**. It should be noted, however, that each use case may be implemented by more SEPA instruments than the one presented.** Therefore, a use case listed in the table below should not be interpreted as the class-type representative of the mobile payment concerned. Moreover, since only a few use cases have been provided in section 3.1, not all categories represented in Table 1 have been covered.

		SEPA Credit Transfer	SEPA Direct Debit (Mandate)	SEPA for Card Payments
Contactless	**P2P**			
	P2B	Pay for Train to Work		Ticket for Football Match Buy Groceries Afternoon refreshment
	B2P			
	B2B			Pay for Business Lunch
Remote	**P2P**	Repay a Friend		
	P2B		Remote Subscription to Online Family Game	Mobile Access to Premium Entertainment
	B2P			
	B2B			

Table 1: Illustration of mobile payments using SEPA instruments.

[1] According to [14], "consumer" means a natural person who, in payment service contracts covered by [14], is acting for purposes other than his trade, business or profession. "Business" is therefore defined as any natural or moral person that is not a consumer.

3.2.2 The Mobile Payment Categories Prioritised by EPC

To maximise the potential and overall benefits of mobile payments, EPC is committed to facilitate a quick market adoption. As a part of this strategy, EPC conducted a market study in 2008 to prioritise its work in the mobile payments area. Based on the following evaluation criteria: business and economic aspects, infrastructure and go-to-market, and, last but not least, market potential. Subsequently, the EPC Plenary, representing all the member banks and payment institutions, selected the following categories in order of priority:

1. Contactless SEPA Card Payments: P2B and B2B;
2. Remote SEPA Card Payments: P2P, P2B and B2B;
3. Remote SEPA Credit Transfers: P2P, P2B and B2B.

Therefore, the following chapters of this white paper deal with these categories only. In particular, the first release of the present document will, besides a general overview on all categories, treat contactless card payments in detail. The next release of this document will also include more detail on both types of remote payments.

3.3 Use cases for Mobile Payments

This section further elaborates on the use cases for mobile payments introduced in the previous sections. It should be noted that for each use the user experience described is only one illustrative example since many different implementations are possible for each use case. Wherever aspects of the mobile phone user interface are mentioned they are also purely illustrative. Further implementation aspects will be elaborated in the upcoming "SEPA Mobile Payment Guidelines".

3.3.1 Mobile Contactless SEPA Card Payments

This section describes a generic Person to Business (P2B) SEPA mobile contactless card payment, irrespective of the type of card used (credit, debit, etc). B2B is implemented if the card holder is a business.

3.3.1.1 Tap and Go

The scenario presented in Figure 4 depicts a possible checkout procedure at a groceries store for a low-value payment transaction.

Before the scenario commences, the payment service provider customer (the consumer) must have subscribed to the mobile payments service for his/her usual payment card, and selected it as the default payment instrument within the mobile phone wallet configuration menu.

- The merchant will start by entering the transaction amount to the POS terminal (1).
- The customer's mobile phone's preselected payment card will be automatically used for this class of payment. Therefore, to confirm the payment transaction, the customer will only need to tap the mobile phone to the NFC-enabled POS terminal (2).

- Thereafter, the transaction is processed (3) as standard SCP transaction and the merchant is able to check the payment (4). Optionally, it is recommended the mobile phone displays the paid amount to the customer (not shown).

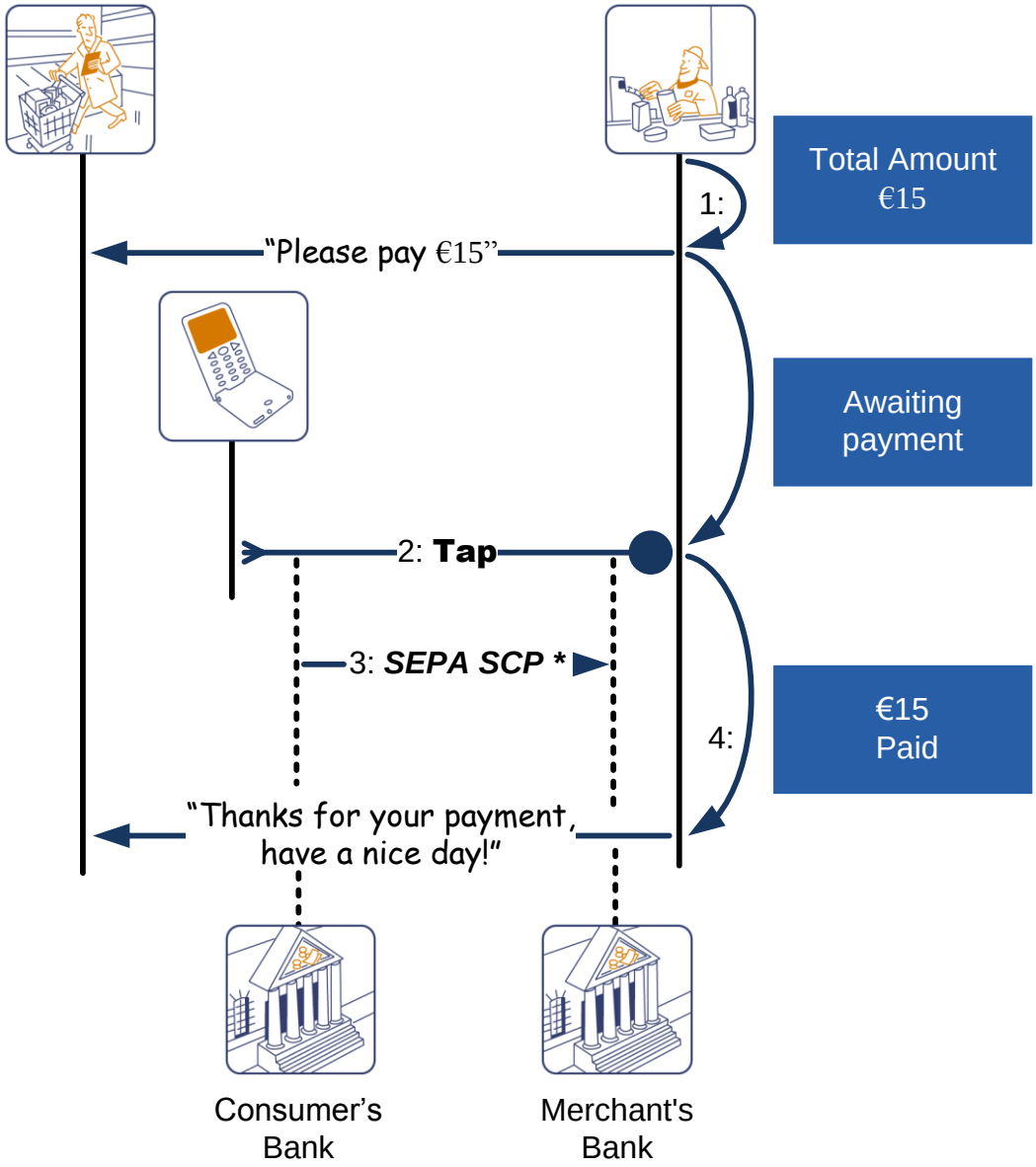

Figure 4: Example of Person to Business Mobile Contactless SEPA Card Payments with Tap and Go.

Note: Protocol steps marked with a * may involve other technical interoperations transparent to the user experience. In the figure, banks are shown as a concrete example of Mobile Payment Service Providers.

Mobile Contactless SEPA Card Payments with Tap and Go – Characteristics	
Category:	Person to Business (P2B). Also applicable to B2B.
Communication type:	Contactless
Payment instrument:	Card - any type
Payment initiation by:	Merchant
Pre-requisites:	• Customer subscribed to Mobile Contactless Payment Services. • Customer pre-selected a payment card as default in his/her mobile. • Merchant with NFC-enabled POS terminal. • Merchant agreement.
Payment confirmation mode:	Tap at NFC enabled POS terminal
Merchant Benefits:	• Highly-efficient payment processing • Co-sales and branding opportunities
Customer Benefits:	• Convenience • Small queues

Table 2: Mobile Contactless SEPA Card Payments with Tap and Go.

3.3.1.2 Double-Tap

The scenario presented in Figure 5 depicts a possible checkout procedure at a groceries store for a high-value payment transaction.

Before the scenario commences, the payment service provider customer (the consumer) must have subscribed to the mobile payments service for his/her usual payment card and selected it as the default payment instrument within the mobile phone wallet configuration menu.

- The merchant will start by entering the transaction amount to the POS terminal (1).
- The customer will tap the mobile phone to the NFC-enabled POS terminal (2).
- The mobile phone's preselected payment card will be automatically used for the payment. Therefore, to confirm the payment transaction, the customer will only need to enter a Personal Code - see *Note* (3) onto the mobile phone and tap the mobile phone a second time (4).
- The transaction is processed (5) as standard SEPA SCP transaction and the merchant is able to check the payment (6).

Note: For security reasons the customer's authentication code denoted as "Personal Code" in this scenario shall not be the same as the card PIN used for conducting contact-based card payment transactions. Further guidance will be provided in the "Mobile SEPA Contactless Card Payments Implementation Guidelines".

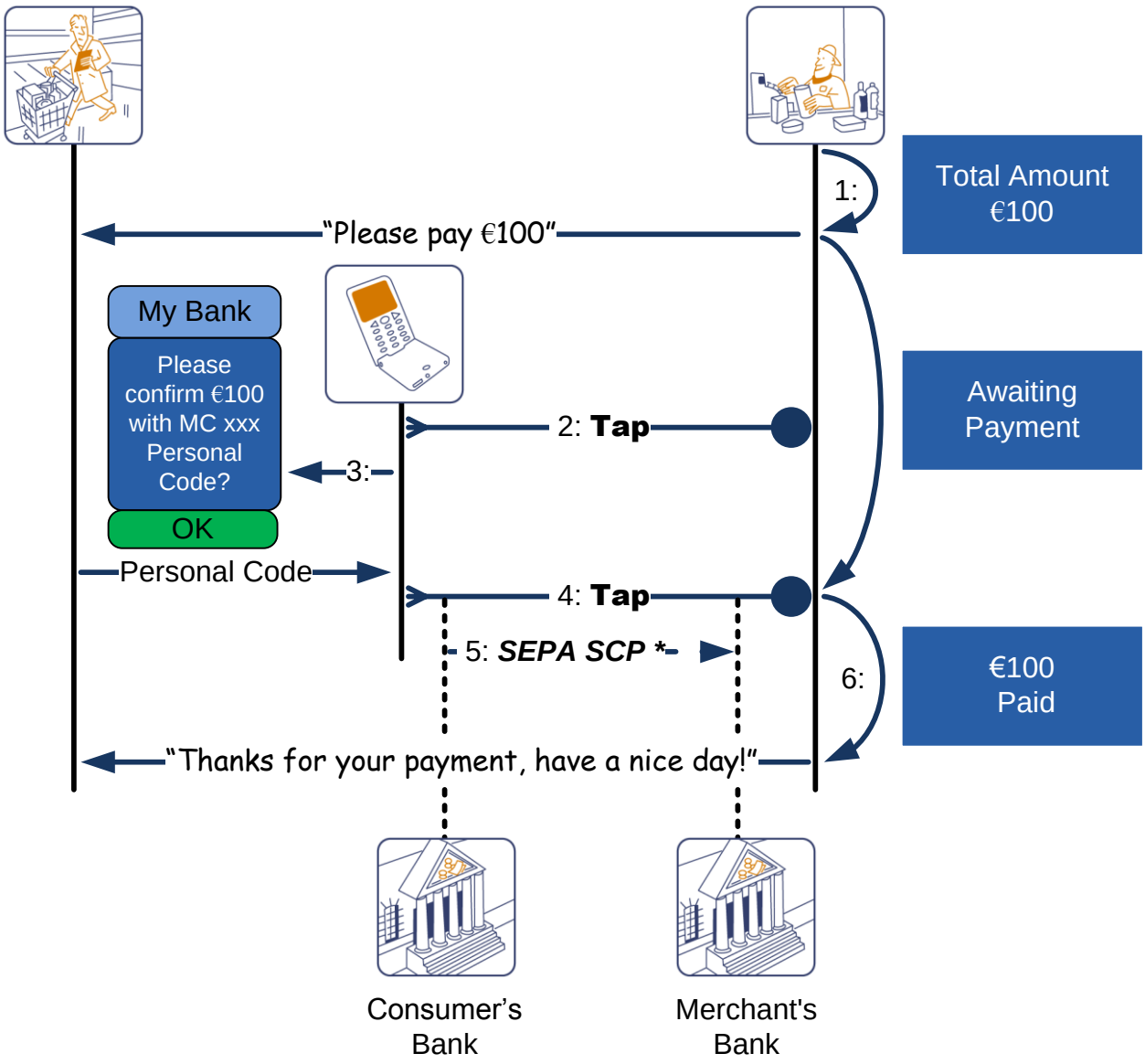

Figure 5 : Example of Person to Business Mobile Contactless SEPA Card Payment with Double-Tap.

Note: Protocol steps marked with a * may involve other technical interoperations transparent to the user experience. In the figure, banks are shown as a concrete example of Mobile Payment Service Providers.

Mobile Contactless SEPA Card Payments with Double Tap – Characteristics	
Category:	Person to Business (P2B). Also applicable to B2B.
Communication type:	Contactless
Payment instrument:	Card - any type
Payment initiation by:	Merchant
Pre-requisites:	• Customer subscribed to Mobile Contactless Payment Services. • Customer pre-selected a payment card as default in his/her mobile. • Merchant with NFC-enabled POS terminal. • Merchant agreement.
Payment confirmation mode:	• Personal Code with confirmation tap at NFC enabled POS terminal
Merchant Benefits:	• Efficient payment processing • Co-sales and branding opportunities
Customer Benefits:	• Convenience • Small queues

Table 3: Mobile Contactless SEPA Card Payments with Double Tap.

3.3.2 Mobile Remote SEPA Card Payments

This section describes a generic person to business (P2B) SEPA mobile remote card payment, irrespective of the type of card used (credit, debit, etc). B2B is implemented when the card holder is a business.

It is assumed that the mobile phone has a secure element enabled for mobile remote SEPA card payments. Also, depending on the final implementation technology, the merchant may have to implement dedicated functionality to:

- recognise the mobile phone as enabled for mobile remote SEPA card payments,
- perform protocol interactions with the mobile phone and the rest of the card payments infrastructure.

3.3.2.1 Single-device Remote Payment and Service Access

In this scenario, illustrated in Figure 6, the customer (the consumer) will use his/her mobile phone to conduct a payment to an Internet merchant, which is providing mobile content (e.g. blockbuster movie).

The properties of this protocol-flow example are similar to those of remote SEPA card payments using a Personal Computer (PC) over the Internet, including authentication of customer, merchant, issuer and acquirer. These protocols are further enhanced by leveraging the existence of the secure element, in areas such as user friendliness and customer authentication.

Note that, while the protocol-flow example included in this section is based on the "Pull mode"[2], other implementation choices exist, and future editions of this document will also include examples based on "Push mode".

Before the scenario commences, the payment service provider customer must have subscribed to the mobile payments service for his/her payment cards (at least one) and enabled them for conducting remote payments within the mobile phone wallet configuration menu.

- While browsing the Internet with his/her mobile phone (also known as mobile Internet), the customer will start by navigating to the check-out section of the merchant's web site (1).
- The merchant's web site will recognise that the mobile phone is enabled for remote payments (2) and decides to offer this payment option to the customer (3).
- Immediately after, the customer receives a payment request on his/her mobile phone display (4), including the transaction amount, the merchant's trusted identification, the service description and a list of supported payment cards already embedded in the mobile phone.
- The customer selects one of the matching embedded cards in his/her mobile phone to make the payment (5). The customer confirms this by introducing her/his dedicated remote payment Personal Code - see *Note* (7).
- The actual SEPA Card Payment is performed as a standard SCP transaction (8) and the merchant will receive notification that the transaction has been carried successfully (9).
- Finally, the merchant will provide the requested premium service to the customer (10).

Note: For security reasons the customer's authentication code denoted as "Personal Code" in this scenario shall not be the same as the card PIN used for conducting contact-based card payment transactions. Further guidance will be provided in the "Mobile SEPA Contactless Card Payments Implementation Guidelines".

[2] Protocols whereby the mobile phone initiates the request (e.g. HTTP request) are referred to as "pull" models. This is opposed to protocols whereby the initial request originates from the merchant's backend (e.g. SMS), which is referred to as "push" models.

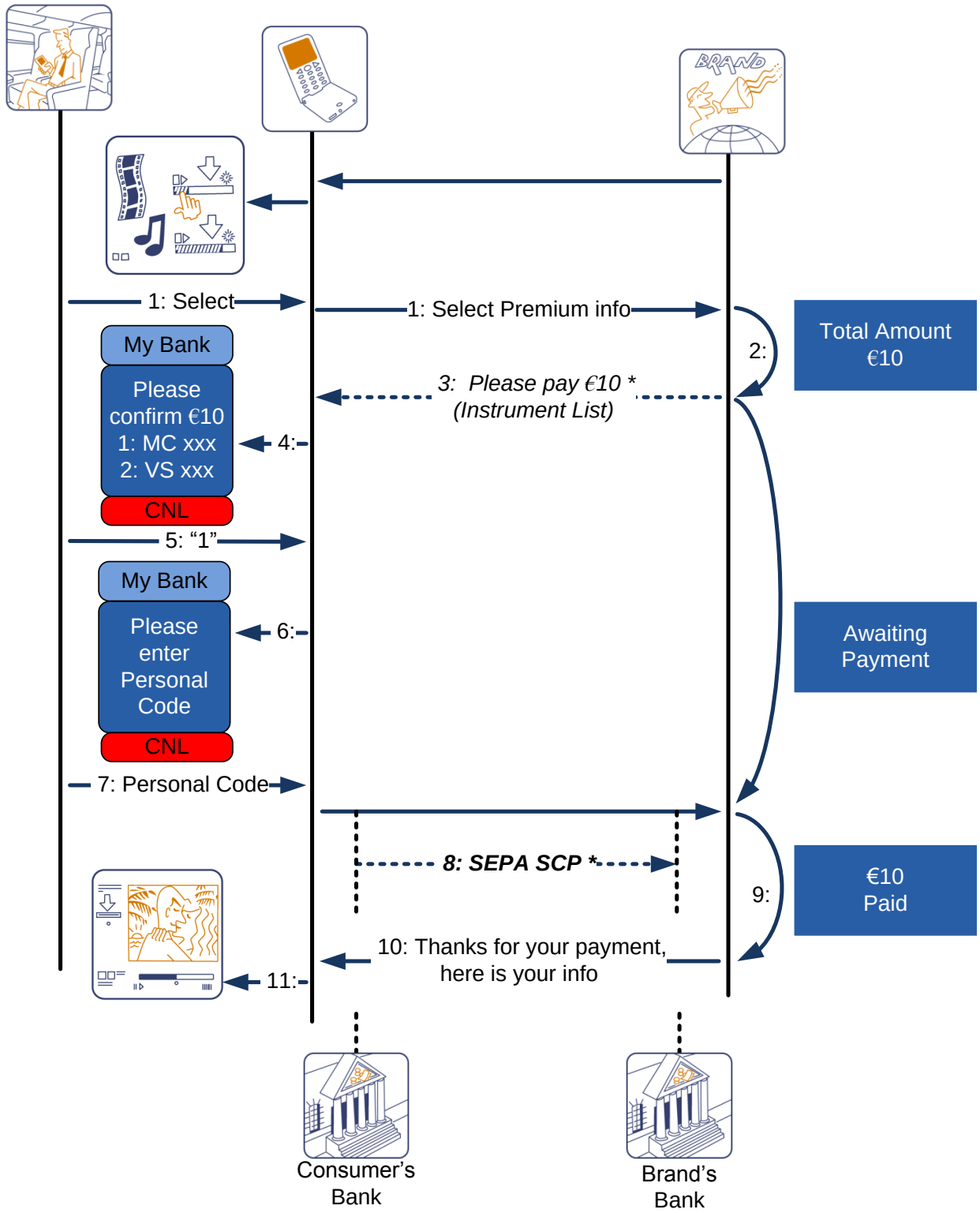

Figure 6: Example of Person to Business Mobile Remote SEPA Card Payment.

Note: Protocol steps marked with a * may involve other technical interoperations transparent to the user experience. In the figure, banks are shown as a concrete example of Mobile Payment Service Providers.

Mobile Remote SEPA Card Payments (Single Device) – Characteristics	
Category:	Person to Business (P2B). Also applicable to B2B.
Communication type:	Remote
Payment instrument:	Card - any type
Payment initiation by:	Merchant (after customer navigation to checkout)
Pre-requisites:	• Customer subscribed to mobile remote payment services • Card enabled by customer for remote payments. • Merchant agreement.
Payment confirmation mode:	Personal Code
Merchant Benefits:	• Lower customer dropouts at checkout stage • Lower risk exposure
Customer Benefits:	• Convenience, mobility • Security

Table 4: Mobile Remote SEPA Card Payments (Single Device).

3.3.2.2 Multi-device Remote Payment and Service Access

In this scenario, illustrated in Figure 7, the customer (the consumer) will use his/her mobile phone to conduct a payment to a mobile Internet merchant providing its services through another device (e.g. a game console).

Before the scenario commences, the payment service provider customer must have subscribed to the mobile payments service for his/her payment cards (at least one) and enabled them for conducting remote payments within the mobile phone wallet configuration menu.

- After selecting the service for which payment it is required, the customer will have the option to give the Internet merchant his mobile phone number or any other identification (3).
- Immediately after, the customer receives a payment request on his/her mobile phone display (4), including the transaction amount, the merchant's trusted identification, the service description and list of supported payment cards already embedded in the mobile phone.
- The customer selects one of the matching embedded cards in his/her mobile phone to make the payment. The customer confirms by introducing her/his dedicated remote payment Personal Code - see *Note* (5).
- The actual SEPA Card Payment (SCP) is performed as a standard SCP transaction (6) and the merchant will receive notification that the transaction has been carried successfully (7). Finally, the merchant will provide the requested premium service to the user (8).

Note: For security reasons the customer's authentication code denoted as "Personal Code" in this scenario shall not be the same as the card PIN used for conducting contact-based card payment transactions. Further guidance will be provided in the "Mobile SEPA Contactless Card Payments Implementation Guidelines".

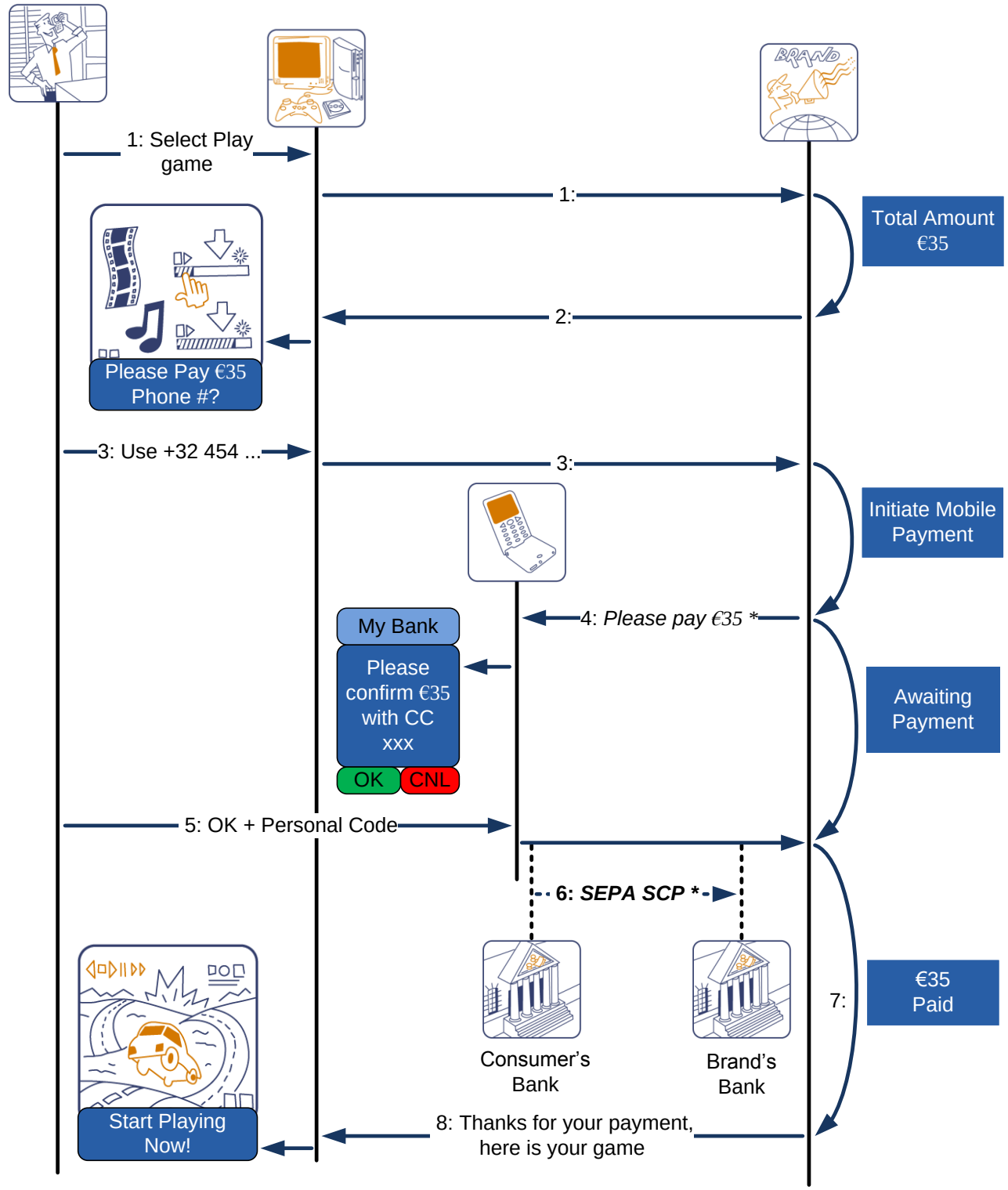

Figure 7: Example of Person to Business Mobile Remote SEPA Card Payment using 2 devices.

Note: Transactions marked with a * may imply other technical interoperations irrelevant to the user experience. In the figure, banks are shown as a concrete example of Mobile Payment Service Providers.

Mobile Remote SEPA Card Payments (Multiple Devices) – Characteristics	
Category:	Person to Business (P2B). Also applicable to B2B.
Communication type:	Remote
Payment instrument:	Card any type
Payment initiation by:	Merchant (after customer navigation to checkout and introduction of mobile phone number)
Pre-requisites:	• Customer subscribed to mobile remote payment services. • Card enabled by customer for remote payments. • Merchant agreement.
Payment confirmation mode:	Personal Code
Merchant Benefits	• Lower customer dropouts at checkout stage • Lower risk exposure
Customer Benefits	• Convenience, mobility • Security

Table 5: Mobile Remote SEPA Card Payments (Multiple Devices).

3.3.3 Mobile Remote SEPA Credit Transfer

This section introduces several generic examples mobile remote SEPA Credit Transfer (SCT). It is always assumed that the mobile phone(s) of the payer (and payees) has a secure element enabled for mobile remote SCT. Also, depending on the final implementation technology, merchants may have to implement dedicated functionality allowing it to recognize the mobile phone as enabled for mobile remote SCT and to perform protocol interactions with it and the rest of the SCT infrastructure.

Independently of the initiation steps, the actual SCT transaction is always based on the usage of the IBAN and BIC.

3.3.3.1 Person to business – Merchant request

This section describes a generic person to business (P2B) SCT. B2B is implemented if the account holder is a business.

In the scenario illustrated in Figure 8, the customer (the consumer) will use his/her mobile phone to conduct a payment to a merchant upon receiving a payment request message from the said merchant. After receiving this request, the consumer will initiate the SCT transaction.

Before the scenario commences, the payment service provider customer must have subscribed to the mobile payments service for his/her accounts (at least one) and enabled them for conducting remote payments within the mobile phone wallet configuration menu.

- The customer requests a service or product from a merchant, remotely or in person. When doing this, the customer also provides the merchant with his mobile phone number (1).
- The merchant determines the price of the service or product and issues a direct service request to the customer's mobile phone (3) (e.g. via SMS).
- Immediately after this, the customer receives a payment request on his/her mobile phone display (4), including the transaction amount, the merchant's trusted identification, the service description and a list of supported SCT payment instruments already embedded in the mobile phone.
- The customer selects one of the matching SCT payment instruments in his/her mobile phone to make the payment. The customer confirms this by introducing her/his dedicated remote payment Personal Code (5).
- The actual SCT transaction will be initiated (6) and the merchant will receive notification that the transaction has been or will be carried/initiated successfully (7).
- The merchant will provide the requested service or product to the customer (8).
- At some point in the future after step (6) the actual SEPA SCT transaction is executed (10)

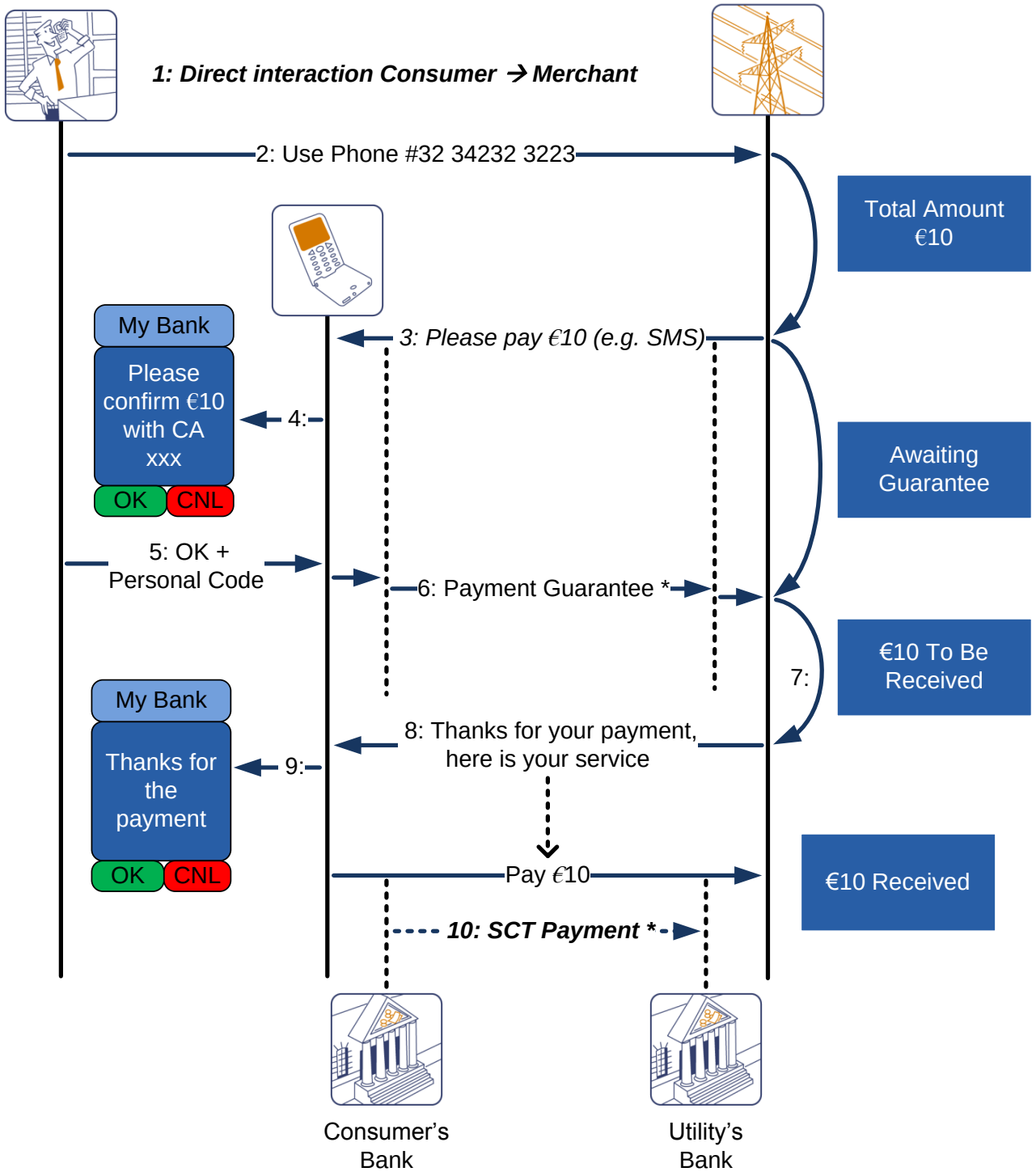

Figure 8: Example of Merchant-initiated Person to Business Mobile Remote SEPA Credit Transfer.

Note: Transactions marked with a * may imply other technical interoperations transparent to the user experience, please see [20] for more details. In the figure, banks are shown as a concrete example of Mobile Payment Service Providers.

Merchant-Request Mobile Remote SEPA Credit Transfer – Characteristics	
Category:	Person to Business (P2B). Also applicable to B2B.
Communication type:	Remote
Payment instrument:	SEPA Credit Transfer
Payment initiation by:	Payee
Pre-requisites:	• Customer subscribed to mobile remote payment services • Merchant agreement.
Payment confirmation mode:	Personal Code
Merchant Benefits	• Lower risk exposure
Customer Benefits	• Convenience, mobility • Security

Table 6: Merchant-initiated Mobile Remote SEPA Credit Transfer.

3.3.3.2 Person to business – Customer request

In a second scenario, illustrated in Figure 9, the customer (the consumer) will use his/her mobile phone to conduct a payment to a mobile Internet merchant.

Before the scenario commences, the payment service provider customer must have subscribed to the mobile payments service for his/her accounts (at least one) and enabled them for conducting remote payments within the mobile phone wallet configuration menu.

- While browsing the Internet with his/her mobile phone (also known as mobile Internet), the customer will start by navigating to the check-out section of the merchant's web site (1).
- The merchant's web site will recognise that the mobile phone is enabled for remote payments (2) and decides to offer this payment option to the customer (3) (e.g. via HTTP reply).
- Immediately after this, the customer receives a payment request on his/her mobile phone display (4), including the transaction amount, the merchant's trusted identification, the service description and a list of supported SCT payment instruments already embedded in the mobile phone.
- The customer selects one of the matching SCT payment instruments in his/her mobile phone to make the payment. The customer confirms this by introducing her/his dedicated remote payment Personal Code (5).
- The actual SCT transaction is initiated (6) and the merchant will receive notification that the transaction has been or will be carried/initiated successfully (7).
- Finally, the merchant will provide the requested premium service to the customer (8).
- At some point in the future after step (6) the actual SEPA SCT transaction is executed (10)

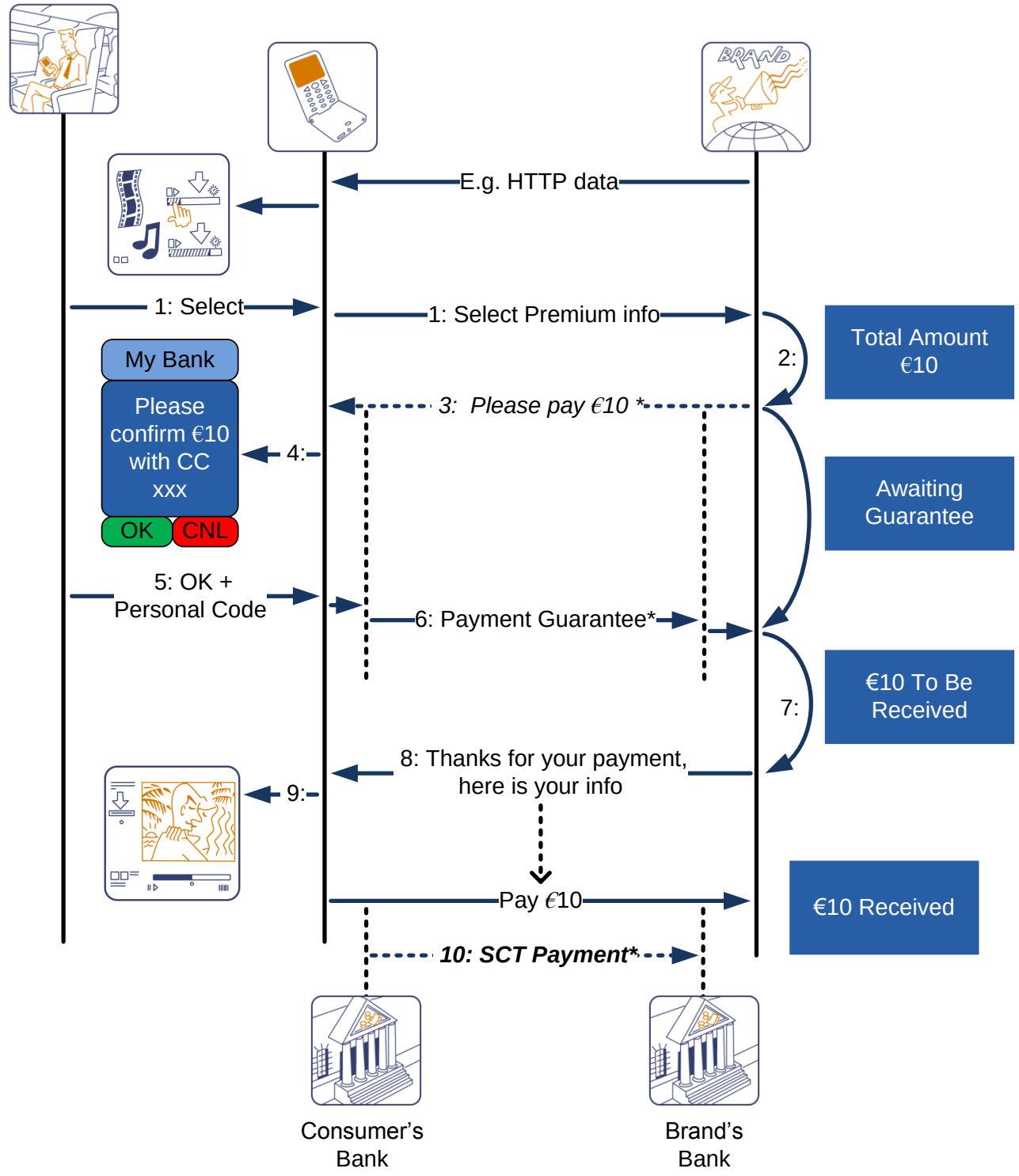

Figure 9: Example of customer-initiated Person to Business Mobile Remote SEPA Credit Transfer.

Note: Transactions marked with a * may imply other technical interoperations transparent to the user experience. In the figure, banks are shown as a concrete example of Mobile Payment Service Providers. The reader is referred to [20] for more details.

Customer Request - Mobile Remote SEPA Credit Transfer – Characteristics	
Category:	Person to Business (P2B). Also applicable to B2B.
Communication type:	Remote
Payment instrument:	SEPA Credit Transfer
Payment initiation by:	Payer (after customer navigation to checkout)
Pre-requisites:	• Customer subscribed to mobile remote payment services • Merchant agreement.
Payment confirmation mode:	Personal Code
Merchant Benefits	• Lower customer dropouts at checkout stage • Lower risk exposure
Customer Benefits	• Convenience, mobility • Security

Table 7: Mobile Remote SEPA Payments (Single Device).

3.3.3.3 Person to Person

Figure 10 introduces a possible example of user experience for an SCT payment initiated by a mobile phone where a first payment service provider customer (payer) wants to make a personal payment to a second payment service provider customer (payee) with his/her mobile phone. Payer and payee may be customers of different payment service providers.

Before the scenario commences, both payer and payee must have subscribed to the mobile payments service for their current accounts (at least one) and enabled them for conducting and receiving remote payments within the mobile phone configuration menu.

- The payer starts by opening the mobile phone payment application (1).
- The payer then introduces the mobile phone number of the payee (2) (alternatively this information could be obtained from the mobile phone's contact book) and the amount to be paid (3).
- The payer's mobile phone contacts the payer's bank to obtain the destination account information from the payee's phone number (4). This could be done by, e.g. an intermediary directory service.
- The payer's mobile phone display shows the payee registered identity information (if pre-authorised by the payee) and the request containing the amount (5). The payer will finally confirm by introducing the payment Personal Code - *see Note* (6).
- Optionally, once the SEPA Credit Transfer initiation has been performed (7), the payee (8) may be notified of the transaction through the mobile phone.

Note: For security reasons the customer's authentication code denoted as "Personal Code" in this scenario shall not be the same as the card PIN used for conducting contact-based card payment transactions. Further guidance will be provided in [15].

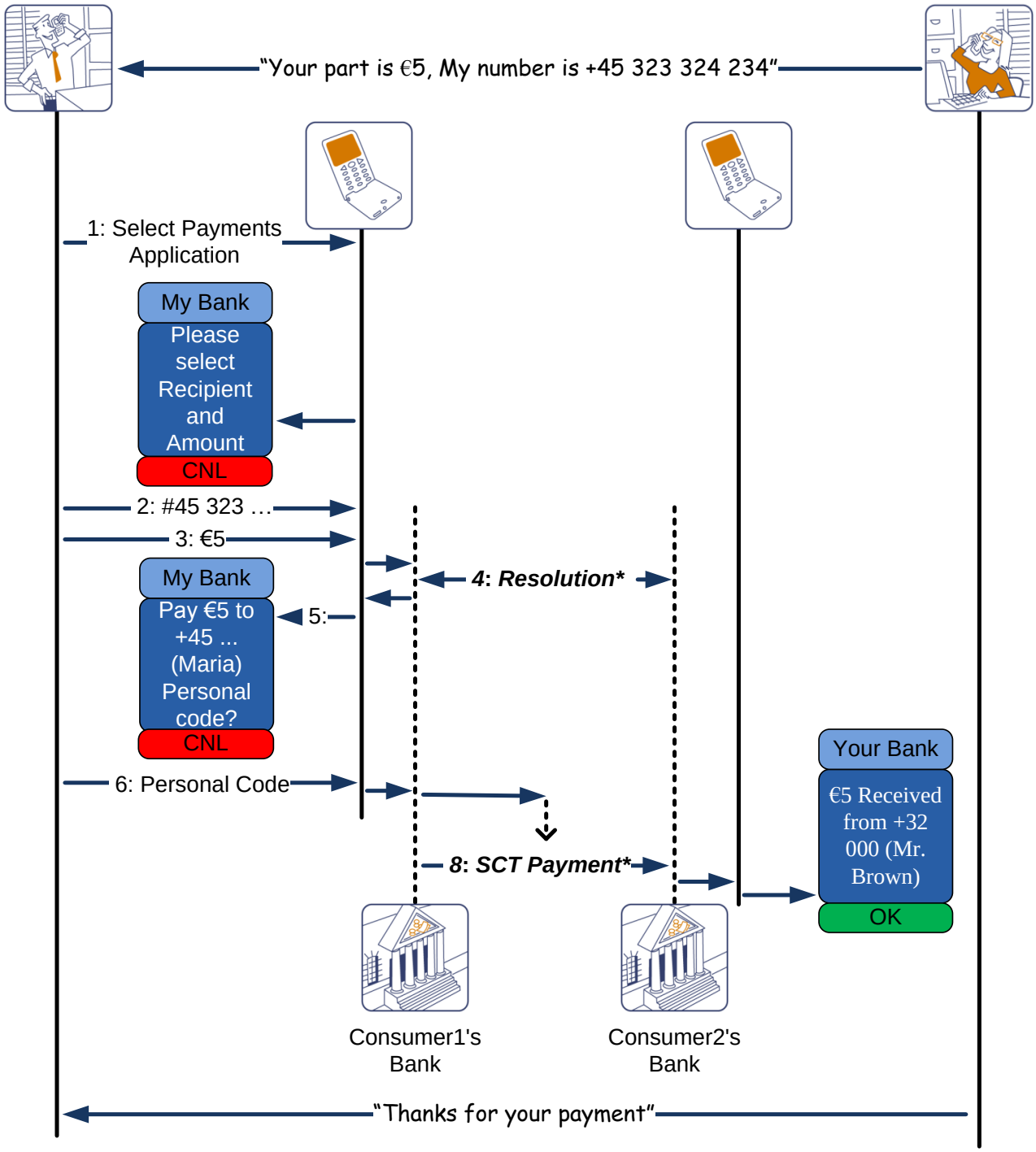

Figure 10: Example of Person to Person Mobile Remote SEPA Credit Transfer.

Note: Transactions marked with a * may imply other technical interoperations irrelevant to the user experience. In the figure, banks are shown as a concrete example of Mobile Payment Service Providers. The reader is referred to [20] for more details.

Person to Person Mobile Remote SEPA Credit Transfer – Characteristics	
Category:	Person to Person (P2P). Also applicable to P2B.
Communication type:	Remote
Payment instrument:	Credit transfer
Payment initiation by:	Payer
Pre-requisites:	Payer and payee subscribed to mobile remote payment services for their respective current accounts.
Payment confirmation mode:	Personal Code
Customer Benefits	• Convenience, mobility • Less cash handling

Table 8: Person to Person Mobile Remote SEPA Credit Transfer.

3.4 Secure Subscription to Mobile Payment Services

The use cases illustrated through this section are not based on the SEPA instruments and they are not subject to standardisation by EPC. They are only introduced here to exhibit how subscriptions to mobile payment services can be easily and conveniently achieved. It should be noted that, thanks to the specific properties of mobile devices, the elapsed time from a customer's service subscription to the execution of the first payment transaction can be reduced to a few minutes.

The registration and provisioning of a mobile payments application needs to be executed in a secure environment. To make it as easy as possible for customers to get access to a mobile payment application, it is important to leverage the regular (secure) applications that he/she is already using.

Please refer to [2] for concrete recommendations on implementing customer registration services while achieving compliance with European Payment Services Directive [14].

3.4.1 Remote Subscription

In this scenario, illustrated in Figure 11, a payment service provider's customer (the consumer) subscribes to mobile payment services via an existing payment service using the web. In this way the customer is already authenticated and working within a secure environment.

This scenario makes the following assumptions:

- The current contract between the customer and payment service provider allows for an e-banking based subscription to new service extensions;
- The mobile phone has the necessary technical capabilities to conduct the desired type of mobile payment services.

The scenario could be conducted as follows:

- The user will first authenticate to the payment service provider as part of the usual e-banking session establishment. Then the user will initiate the mobile services subscription by entering his/her mobile phone number and indicating which particular service he/she wants to use (1) (2).
- Subsequently the payment service provider will check the technical eligibility of the mobile phone (including the SIM or/any other S.E.) directly or by using the services provided by a third party (3).
- The customer will receive an SMS from the payment service provider on his mobile phone to signal this (4).
- As soon as he/she opens the SMS and confirms (5) he/she wants to start the service with the mobile phone that is receiving the message, the service is fully provisioned (6). Once the service is provisioned the mobile phone's display provides confirmation to the customer.

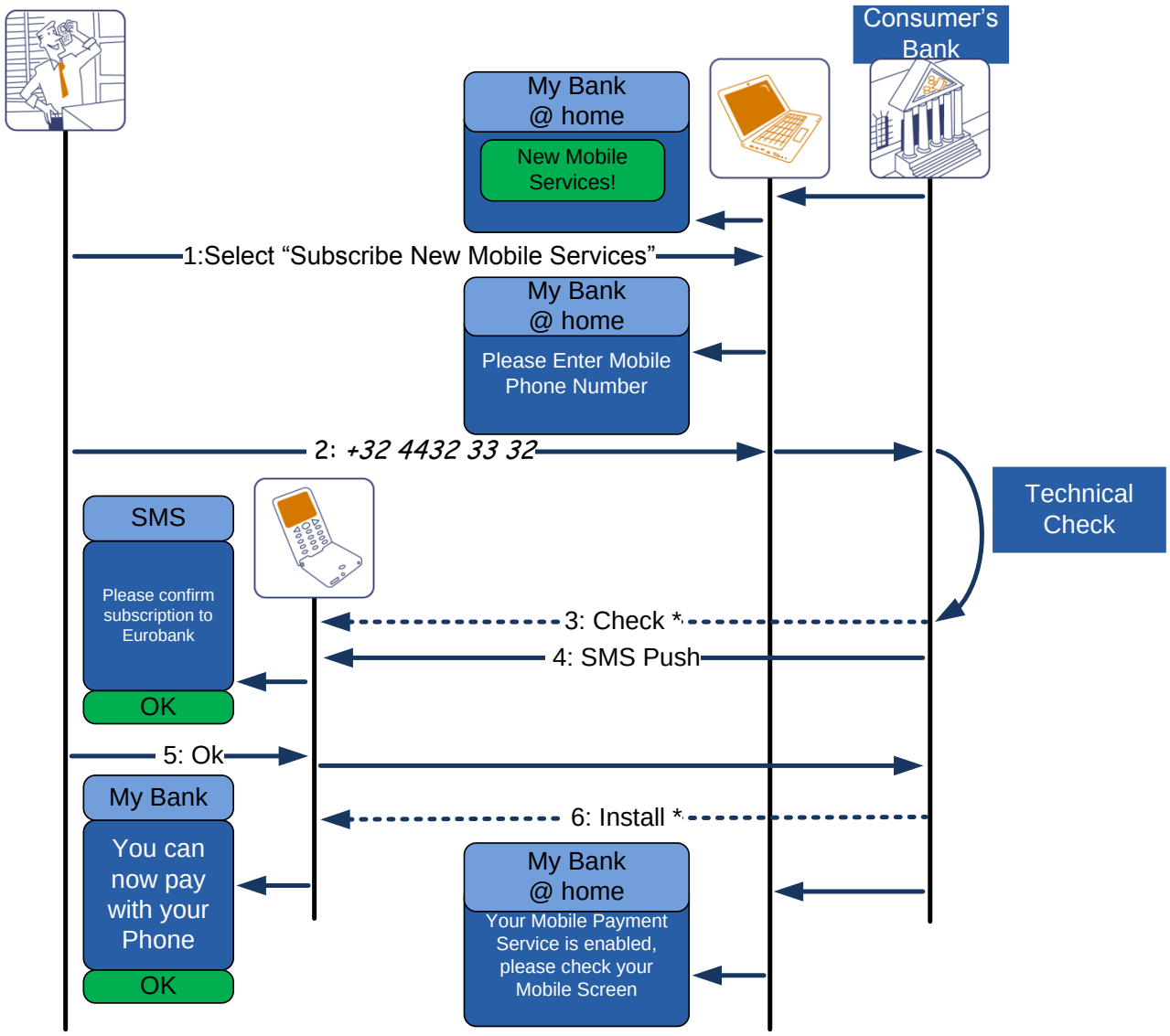

Figure 11: Example of Remote Subscription to Mobile Payment Services.

Note: Transactions marked with a *may imply other technical interoperations irrelevant to the user experience. In the figure, a bank is shown as a concrete example of Mobile Payment Service Provider.

3.4.2 Subscription with Self-Service Device

In this scenario, illustrated in Figure 12, a payment service provider's customer (the consumer) subscribes to mobile payment services via a self-service device (e.g., ATM). In this way the customer is already authenticated and working within a secure environment.

This scenario makes the following assumptions:

- The current contract between the customer and payment service provider allows for an ATM-based subscription to new service extensions;
- The mobile phone has the necessary technical capabilities to conduct the desired type of mobile payment services.

The scenario is conducted as follows:

- The user will first authenticate to the ATM as part of the usual session establishment. Then the customer initiates the subscription by entering his/her mobile phone number and indicating which service he/she wants to use (1) (2).
- The payment service provider will then check the technical eligibility of the mobile phone (including the SIM or/any other S.E.) directly or by using the services provided by a third party (3).
- The customer will receive an SMS from the payment service provider on his mobile phone to signal this (4).
- As soon as he/she opens the SMS and confirms (5) he/she wants to start the service with the mobile phone that is receiving the message, the service is fully provisioned (6). Once the service is provisioned the mobile phone's display provides confirmation to the customer.

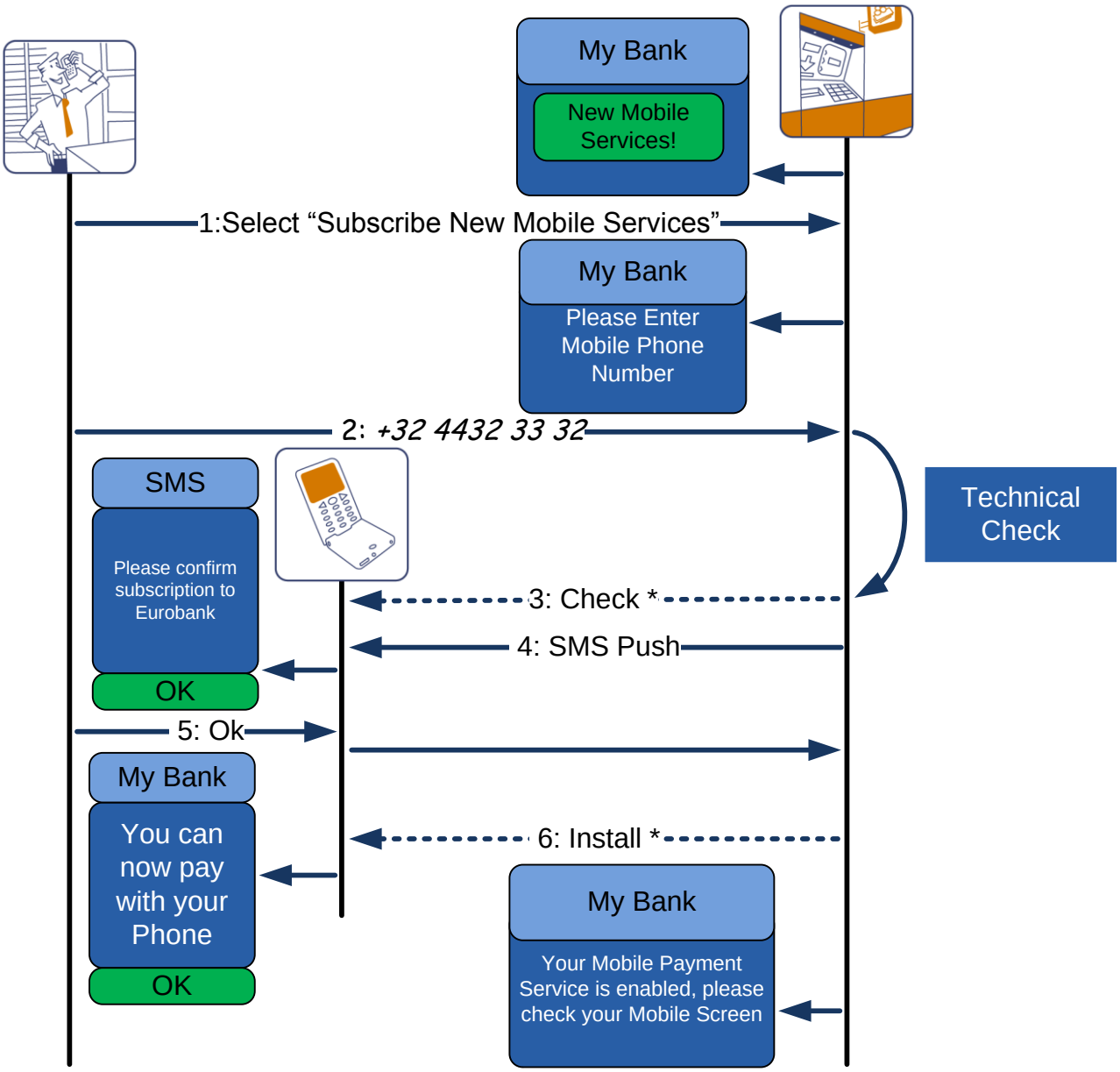

Figure 12: Example of ATM subscription to mobile payment services scenario.

Note: Transactions marked with a * may imply other technical interoperations irrelevant to the user experience. In the figure, a bank is shown as a concrete example of Mobile Payment Service Provider.

3.4.3 Subscription at the Bank's branch

In this scenario, illustrated in Figure 13, the subscription to mobile payment services is performed when the payment service provider's customer (the consumer) visits his/her bank branch.

This scenario makes the following assumptions:

- The mobile phone has the necessary technical capabilities to conduct the desired type of mobile payment services.

The scenario is conducted as follows:

- After notifying the branch clerk of his/her intention to subscribe to the mobile payment services (1), the customer will provide the mobile phone number to be enrolled as part of the registration information (2).
- The bank will then check the technical eligibility of the mobile phone (including the SIM or/any other SE) directly or by using the services provided by a third party (3).
- The new functionality is enabled remotely on the mobile phone (4), and the customer will simply discover a new payment application installed in his/her mobile phone.

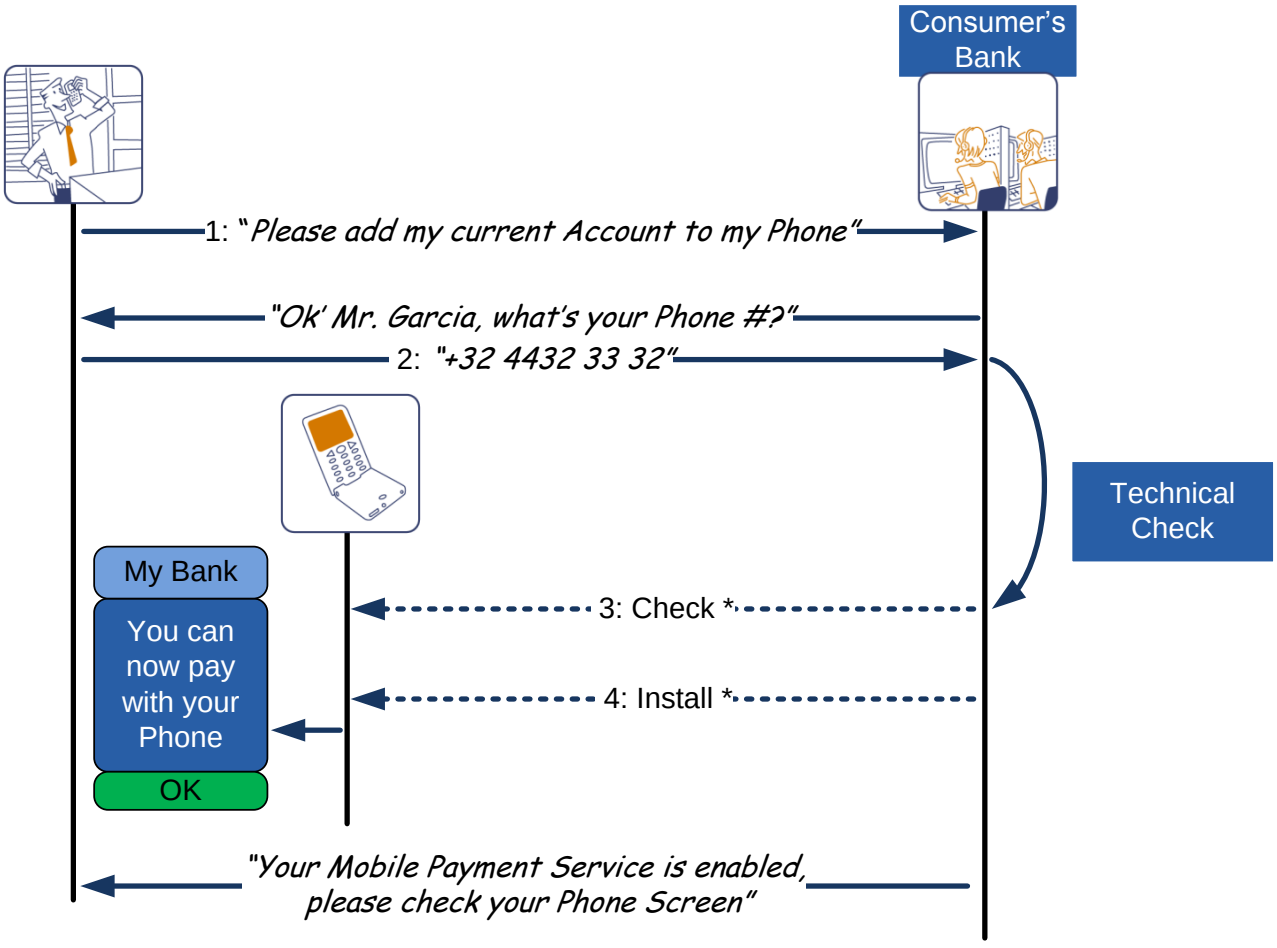

Figure 13 : Example of in-person Mobile Payment Service subscription use case.

Note: Transactions marked with a * may imply other technical interoperations irrelevant to the user experience. In the figure, a bank is shown as a concrete example of Mobile Payment Service Provider**.**

4 Mobile Contactless Card Payments

4.1 Introduction to Mobile Contactless Card Payments

This chapter provides an in-detail presentation of mobile contactless SEPA card payments, which are defined as any SEPA contactless card payment (see [17]) executed by a payment service provider's (called "card issuer" in the rest of this chapter) customer using a dedicated mobile contactless payment application over NFC. The mobile contactless payment application is provided by the card issuer and is, for example, loaded onto the secure element, which is independently provided by secure element issuer. Regardless of the secure element used, the introduction of the mobile contactless technology should aim to achieve the same security level as for the existing SEPA card payments.

As illustrated in Figure 14, the main parties involved in the transactions based on mobile contactless card payments do not differ from a "classical" SEPA card payment. The payment transaction is performed by reusing the existing SEPA contactless card payments accepting devices, while the back-end and transaction infrastructure will be those already used for SEPA card payments (see [17]).

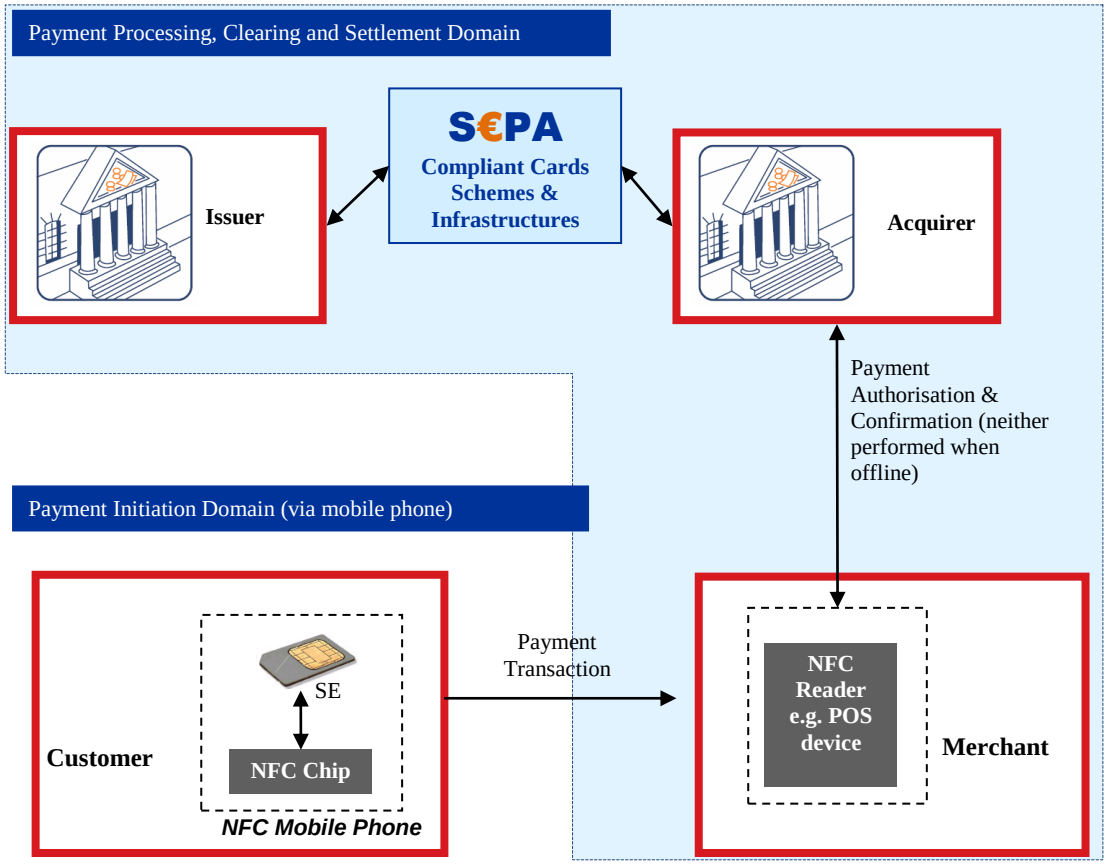

Figure 14: Mobile Contactless Card Payment Transaction. Elements within the blue shadedarea are similar to Contacless Card Payments.

The reader is referred to section 3.3.1 for a use case-oriented description of mobile contactless card payment transactions.

4.1.1 High Level Guiding Principles

The following guiding principles are used by EPC to execute its vision for mobile contactless SEPA card payments:

- Mobile contactless SEPA card payments should build on existing SEPA payments rulebooks and the SEPA Cards Framework.

- The payment service provider (or card issuer) brands must be supported in user interfaces on the mobile phone. The card issuer is responsible for the definition its own presentation (graphical interface) to the customer including brands & logos, card scheme brands, payment type etc..

- Creating ease, convenience and trust for the end-users, (customers and merchants), using a mobile phone to initiate a mobile payment, is regarded as critical for the further development of this area.

- Customers should have the same payment experience when performing a mobile contactless SEPA card payment transaction independent of the location at which the transaction is executed. This includes the interaction with the accepting device (POS).

- Customers should not be bound to a specific mobile network operator or a particular handset and should retain their current ability to switch between card issuers. Customers should also be able to change the mobile phone (provided it meets the technical requirements).

- Customers must be able to make mobile contactless card payments in all SEPA countries regardless of the original country where the contactless payment services were subscribed.

- Customers must be able to use mobile contactless card payment services issued by different card issuers using a single mobile phone, and must be able to select the relevant contactless payment service to be used for a payment transaction.

4.2 Infrastructure

4.2.1 Network & Back-End

4.2.1.1 Payment Transactions

The infrastructure needed during the payment transaction for mobile contactless card payments fully leverages the infrastructure already deployed for card payments. Mobile contactless SEPA card payments will further leverage the investments to be made for acceptance of contactless cards.

4.2.1.2 Provisioning & Management

The mobile contactless SEPA cards payment application is to be installed on a secure element (see section 2.3). This implies that dedicated processes need to be defined for the provisioning and management of the said payment application, which may vary depending on the secure element chosen. It is expected that existing card personalisation systems can be leveraged for the personalisation of the payment application. In order to achieve this, third party providers might be involved, such as the MNOs in the case of the UICC.

4.2.2 Mobile Phones

Within SEPA, all deployed general-purpose mobile phones are either GSM or UMTS (also known as 3G). All UMTS mobile phones have mobile broadband capabilities, and virtually all new GSM mobile phones currently sold also support GPRS or EDGE, which also provide seamless access to Internet, albeit with a thinner bandwidth.

Mobile phones can be efficiently managed remotely from the mobile network infrastructure by either using the standard networking protocols issued by ETSI and GSMA, or application-specific protocols built on top of standard Internet access protocols (HTTP). If the mobile network infrastructure is used, access (and cost) is fully transparent to the end user.

Mobile phone handsets are constantly being developed and feature an ever-increasing number of capabilities. Modern phones known as "smart-phones" are based on general-purpose (open) computing platforms capable of achieving very complex tasks, they forester colour screens in an ever-increasing size, and allow for PC-like Internet access capabilities. Significantly, the smart-phone is the only category of mobile device that is currently growing in market share, and at a remarkable pace [7].

In parallel, the usage of stand-alone contactless cards is finally coming of age and mass deployment of contactless card-based services has already started for applications such as ticketing. Many deployments of payments solutions using contactless cards exist worldwide and the EPC is currently working with the key stakeholders to standardise contactless cards protocols for the SEPA card payments framework.

NFC is just a full backwards-compatible extension of the contactless card protocols[3]. NFC-enabled phones can interact with standard RFID readers (e.g. POS) and with other NFC-enabled devices. Accordingly, they have the potential to fully leverage any existing infrastructure for card-based contactless payment services. Mass-deployment of NFC-enabled mobile phones in SEPA is expected shortly.

Therefore, it is reasonable to assume that, in SEPA, present and future payment applications can effectively rely on a wide deployed base of mobile phones featuring rich remote management capabilities, Internet access, and high resolution colour screens capable of sustaining an adequate user experience.

4.2.3 End-User Interface

[3] The main difference is that a contactless card is said to communicate "passively" i.e. without needing its own power source, while a NFC-enabled mobile phone can use its batteries for extra functionality.

Even if the most advanced smart phones boast "great" colour displays and touch-based interfaces, the user experience remains strongly challenged by the necessarily-small form factor. For example, the mobile phone form factor effectively limits the amount of information that can be displayed at any given time and the ability of the user to enter complex text.

Therefore, the main challenge for customer adoption of contactless mobile payments is the availability to provide for an extremely easy-to-use, consistent user experience across all the supported mobile phone implementations.

EPC will introduce specific assistance to address this topic in the [15] document.

4.2.4 The UICC as the Secure Element

As introduced in section 2.3, the sensitive operations undertaken by the mobile contactless card payments application should be made within a secure element.

Conveniently, all modern GSM mobile phones incorporate the "UICC" (previously SIM), which is a tamper-resistant token owned and provided by the MNOs, which has been fully standardised by ETSI. Whereas the UICC already manages the necessary confidential and cryptographic data to securely identify the user to the mobile network, the UICC can also host said data and applications for entities ("service providers") other than the MNO owning it. Furthermore, this may be done while still preventing the MNO to access any data managed by the said service providers.

Therefore, due to its ubiquity, world-wide standardisation, and security properties, the UICC has been widely chosen by payment service providers as the first selected candidate to host the security-sensitive components of mobile contactless SEPA card payment applications.

Notwithstanding, other types of secure elements are adequate alternatives such as embedded SEs, and micro SD Cards. Annex V – The Secure Element, provides further guidance on these.

The upcoming documents to be issued by the EPC will also treat other secure element alternatives and their associated challenges.

4.2.4.1 Challenges

The leverage of the UICC as the secure element by card issuers introduces several new challenges that must be properly addressed for a successful SEPA-wide deployment:

1. While based on the same technology as for existing payment chip cards, the UICC is not yet certified to the same security levels;
2. Even though they share many industrial players, the personalisation and associated supply-chain infrastructure differs from that of payment chip cards, which will need to be re-certified to attain equivalent security levels;
3. Payment chip cards are currently certified using a monolithic approach, the existing certification methods must be extended to allow for "arbitrary" on-the-field mobile contactless payment application installation.
4. A "firewall" must be built to separate the basic applications (issued by MNOs and/or other service providers, such as ticketing) from the contactless card payment applications in each UICC. The same applies for contactless card payment application from different card issuers.

5. Finally, access to UICC is currently tightly controlled by the (issuing) MNOs. Without further support, card issuers will need to establish commercial relationships and co-implement several business processes with many MNOs simultaneously to attain any significant SEPA-wide deployment.

The challenges 2 and 4 have been addressed in [18], which EPC has jointly developed with GSMA. The following sections aim to elaborate further on the challenges mentioned above while even more detail will be covered in forthcoming documents which will be issued by the EPC.

4.2.5 Mobile Contactless Card Payment Applications

The mobile contactless card payment application implements the payment card functionality within the phone. The actual functions executed by it are subject to the requirements set forth in the EPC Cards Standardisation Volume [17]. The mobile contactless card payment application has direct access to the NFC interface and therefore it communicates directly with the card accepting device. Mobile contactless card payment applications are under the responsibility of the card issuer and should reside on the secure element. Mobile contactless card payments applications are personalised and managed remotely by the card issuer.

Card issuers should be free to compete in their services offering by customising the mobile contactless card payment application, user-oriented configuration functions and the (remote) management operations.

4.2.6 Mobile Contactless Card Payment Application User interface

A mobile contactless card payment application may be supported by complementary applications residing in the mobile phone's "main memory", which are known as "Mobile contactless Card Payment Application User Interface" and they are dedicated to interact with the user. Please refer to section 4.2.3 for more details about specific considerations for these applications. The card issuer is responsible for this application, its security characteristics and the secure communication with the mobile contactless card payment application.

4.2.7 Point of Sale

RFID technology is finally able to realise its promise thanks to the existence of the first deployments of significant geographical size and penetration, such as the Oyster network in Greater London and the stadiums access systems deployed by some major football clubs. However, most of the POS infrastructure is not yet enabled for RFID and this will require further upgrading. This upgrade should include the potential requirements beyond those already defined for contactless SEPA card payments to maximize the effectiveness of those investments. For example, while the requirements for hardware components are expected to be identical, the embedded software may have to be updated for supporting e.g. the adequate handling of "Personal Codes" (see section 3.3.1.2 for an example of usage of Personal Codes for authentication). The EPC is already actively involved on this issue with all the relevant standardisation bodies and stakeholders.

4.2.8 Standardisation and industry bodies

Mobile SEPA contactless card payments require the careful coordination of standards and specifications defined within several disciplines and issued by a heterogeneous group of industry bodies and global organisations. Next to EPC the most relevant are:

- **ISO**

  The International Organization for Standards (ISO) is the world's largest developer and publisher of International Standards. ISO has different committees which specify technical standards used in mobile payments such as standards for integrated circuit cards, communication protocols such as NFC, security mechanisms and is also is involved with mobile payments in ISO TC68. [9]

- **ETSI**

  The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies, including fixed, mobile, radio, converged, broadcast and internet technologies. ETSI defines GSM, UMTS telecommunication protocols and the UICC including all the access protocols. [4]

- **EMVCo**

  EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard and Visa. [3]

- **IETF**

  The Internet Engineering Task Force (IETF) is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF defines the core for all Internet protocols. [8]

- **GlobalPlatform**

  GlobalPlatform (GP) is the leading, international association focused on establishing and maintaining an interoperable and sustainable infrastructure for smart card deployments. Its technology supports multi-application, multi-actor and multi-business model implementations, which delivers benefits to issuers, service providers and technology suppliers. [5]

- **GSMA**

  The GSMA represents the interests of the worldwide mobile communications industry. Spanning more than 200 countries, the GSMA unites nearly 800 of the world’s mobile operators, as well as more than 200 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers, Internet companies, and media and

entertainment organisations. The GSMA is focused on innovating, incubating and creating new opportunities for its membership, all with the end goal of driving the growth of the mobile communications industry. [6]

- **Mobey Forum**

Mobey Forum is a global, financial industry driven forum, whose mission is to facilitate banks to offer mobile financial services through insight from pilots, cross-industry collaboration, analysis, experience-sharing, experiments and co-operation and communication with relevant external stakeholders. [11]

- **NFC Form**

The Near Field Communication (NFC) Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. [13]

4.3 The Business Ecosystem for Mobile Contactless Card Payments

As argued in section 4.2, mobile contactless SEPA card payments need to rely on a series of technical infrastructure elements that are unique to the mobile environment. Of particular interest are the handsets, the UICC and the mobile network operator backend systems intended to manage them. EPC's gap analysis has determined that the current lack of standards for interoperability between card issuers and MNOs constitutes the single biggest barrier to successful commercial deployments. Therefore, EPC has setup a dedicated joint effort with the GSMA to ensure this is done in a uniform and well-coordinated manner across all mobile deployments in SEPA. The main structure of the new ecosystem is depicted in Figure 15, where the new players introduced to support the mobile contactless card payments are highlighted in red-hues.

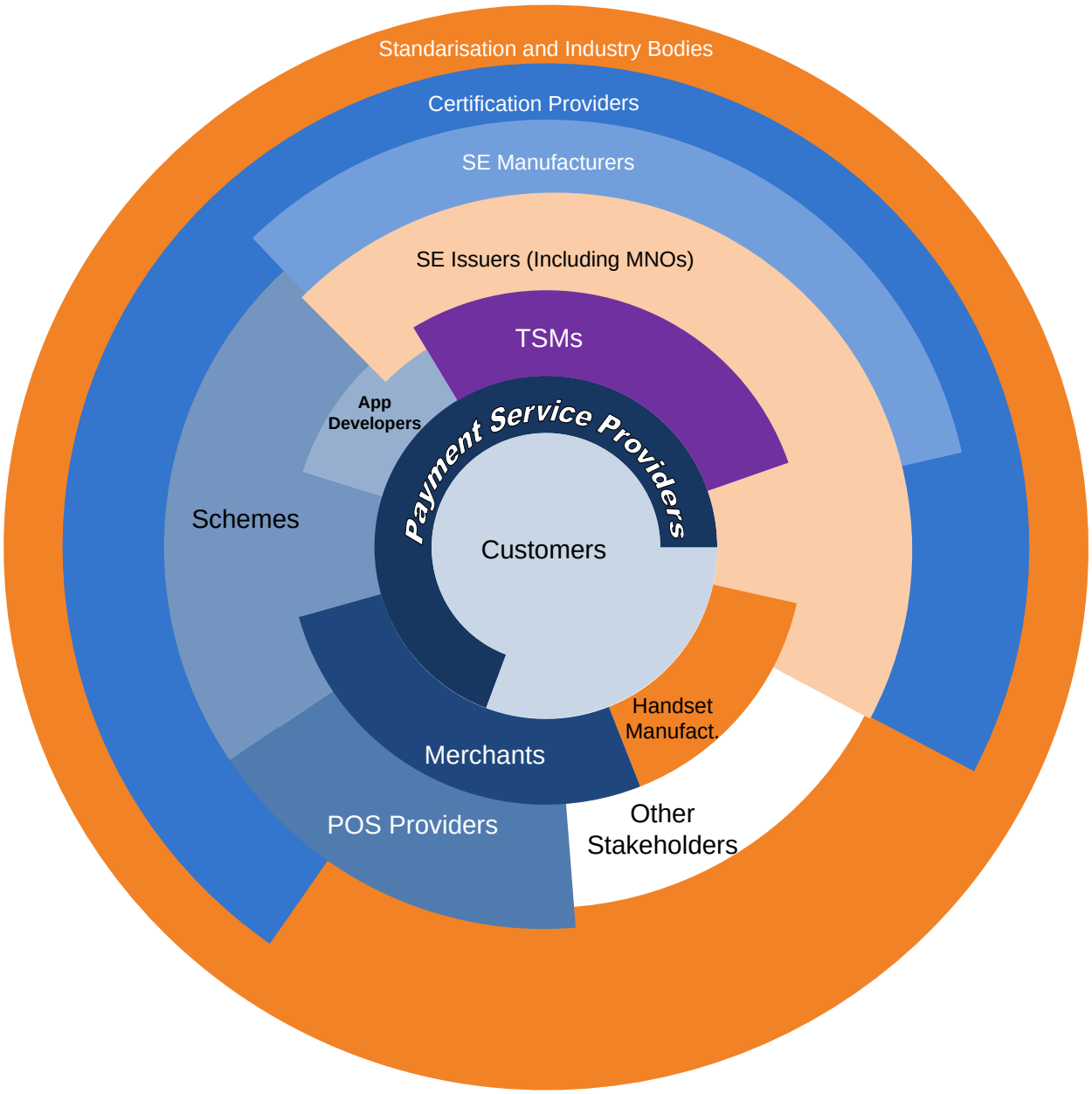

Figure 15: Mobile Contactless SEPA Card Payments Business Ecosystem. Contact points depict major business relationships between players.[4]

Although only minor changes to the existing card payment acceptance infrastructure (network and back-end systems) are expected, merchants and acquirers need to upgrade the existing card accepting infrastructure to enable contactless technology. This can be done in such way that both contactless cards and mobile contactless are dealt with.

Changes to the issuers' infrastructure for mobile contactless SEPA card payment application provisioning are expected. The next sections introduce several new elements supporting issuers in understanding and managing those changes.

[4] This picture is provided only as a reader-friendly overview of the mobile contactless SEPA card payments ecosystem, the relative areas allocated to each actor do not convey any meaning.

4.3.1 New Stakeholders Introduced to the Payments Ecosystem

As introduced above, the most salient stakeholders introduced by mobile contactless card payments are the secure element issuers. These are the MNOs in case of a UICC, the handset manufacturers or card issuers in case of embedded secure element, etc. In case of a UICC, the MNO enables, through its back-end services, the card issuer(s) to securely install and manage remotely their mobile contactless card payment applications.

The "Trusted Service Manager" (TSM) is an optional third party introduced to provide for better scalability when several card issuers must undertake commercial and technical interactions with several secure element issuers. As illustrated in Figure 16, card issuers, TSMs and secure element issuers collaborate to perform the provisioning and management of the secure element-based mobile contactless payment application(s).

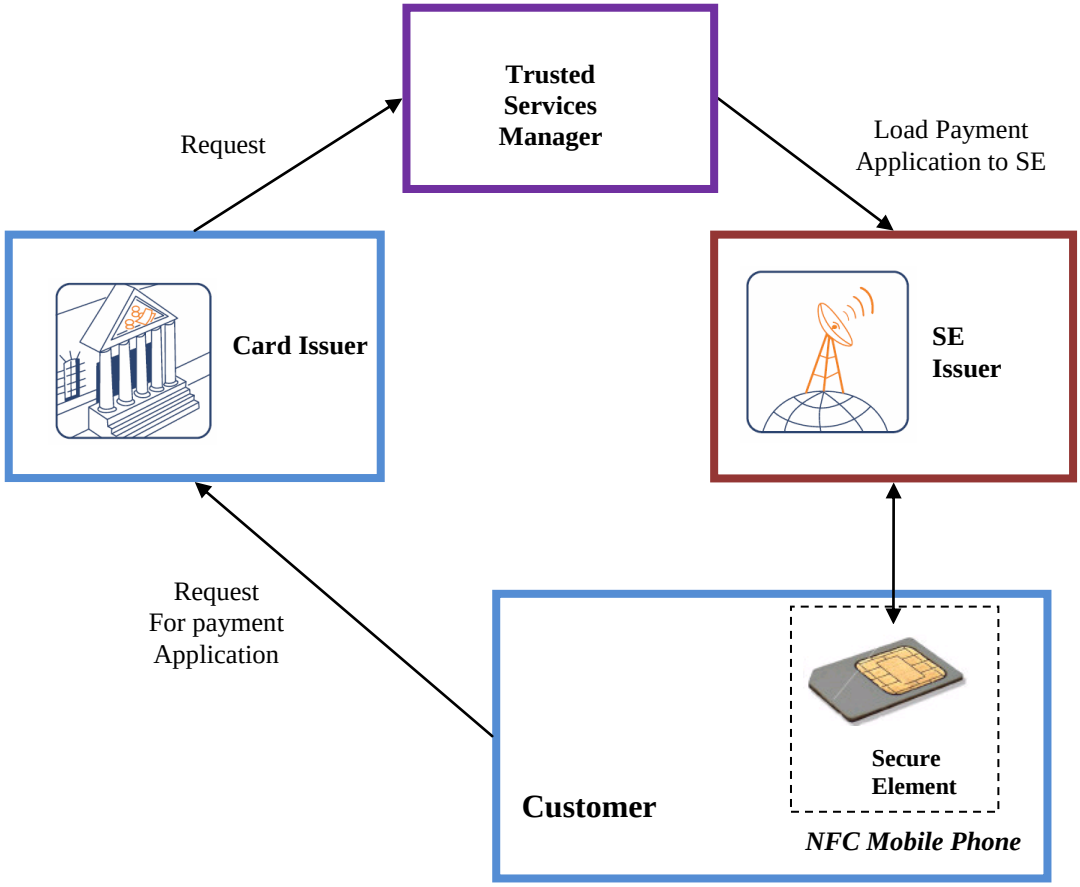

Figure 16: Provisioning of Mobile Contactless Card Payments Applications to a Secure Element.

To facilitate an open ecosystem, many TSMs may exist offering mutually-competing services to both Issuers and secure element issuers.

Other relevant new stakeholders are:

- UICC manufacturers;

- UICC controlling authorities;
- Mobile contactless application developers;
- Handset manufacturers;
- NFC equipment manufacturers;
- Organisations performing certification for UICCs and MCP applications.

4.3.2 Business Models

4.3.2.1 Payment Transaction

Mobile contactless SEPA card payments do not modify in any way the underlying SEPA cards payment transaction. Therefore the business models of the SEPA card payment transactions are unaffected. Please refer to section 4.1 for details.

4.3.2.2 Provisioning and Management

In order to facilitate the introduction of a rich ecosystem of service providers performing TSM functions, EPC and GSMA have prepared a formal partition of the commercial and technical responsibilities involved in the provisioning and management of the mobile contactless payments SEPA card applications [18]. A high-level summary of this partition is illustrated in Figure 17.

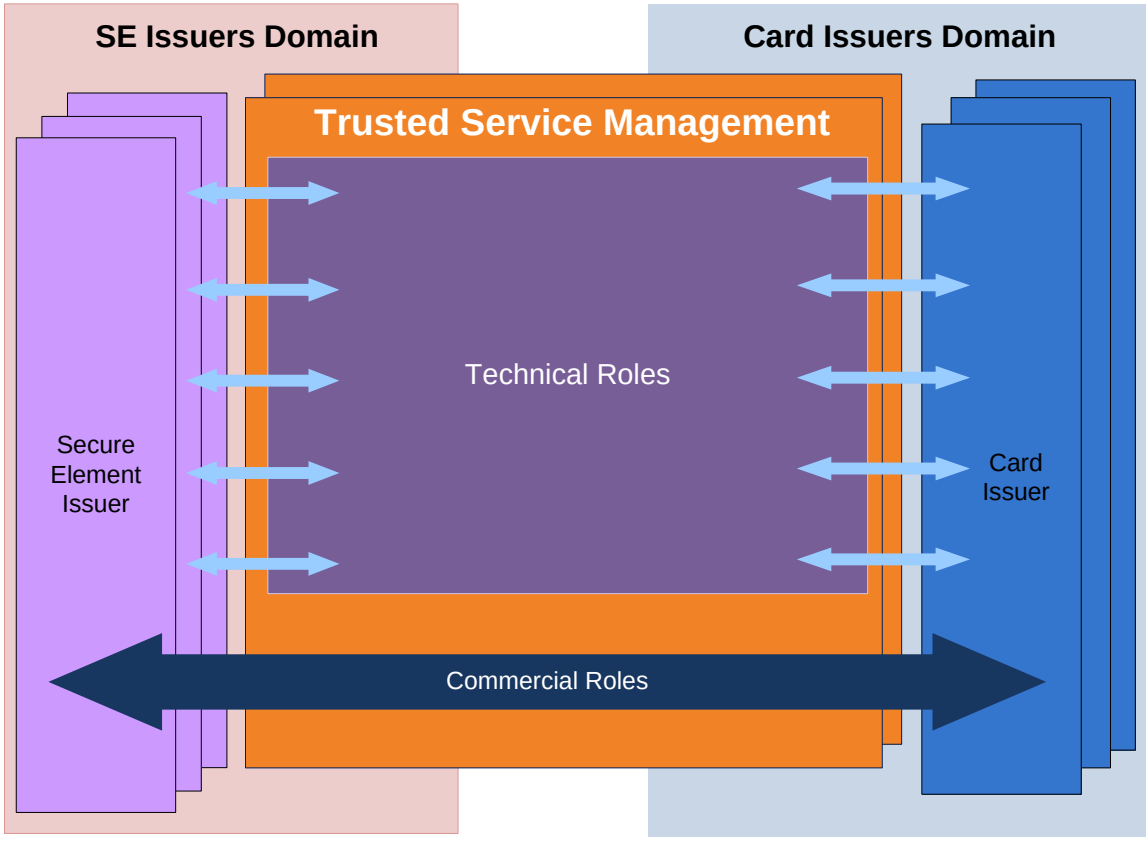

Figure 17: Provisioning & Management overview for contactless mobile SEPA card payments.

Many business and services models are possible by delegating combinations of the different technical and commercial roles to one or more TSMs, including three and four-party business models, please refer to [18] for a detailed introduction.

5 Next steps

The EPC will provide a second edition of this document including a more detailed section on mobile remote payments, similar to the chapter 4 above, for mobile contactless card payments.

As mentioned earlier in this document, it is up to the individual market participants in mobile payments to decide if and when they will implement their services in this area. In order to further support payment service providers wishing to enter the mobile area, EPC will publish forthcoming implementation guidelines both for mobile contactless card payments and mobile remote payments. As stated earlier, the role of EPC is to leverage existing SEPA instruments. These future documents will aim to provide further direction in a number of topics, which are currently not (or not sufficiently) covered by the existing documentation provided by technical standardisation bodies or industry organisations. In particular, EPC will focus on a number of business aspects, such as models and processes. Also, some technical and security topics will be handled in more detail, such as mobile wallet design guidelines, risk and security aspects associated with the usage of the mobile phone and the new players and processes in the mobile ecosystem. In producing these implementation guidelines, EPC will follow the same priorities as with the current white paper.

In the area of provisioning of mobile contactless payment applications, the reader is further advised to consult [18], which provides further guidance on business processes and technical and security requirements.

Annex I – Definitions

- **Acquirer**

A payment service provider accepting mobile payments.

- **Card Issuer**

In the context of chapter 4, a payment service provider acting as issuer of mobile contactless SEPA card payments.

- **Consumer**

A natural person who, in payment service contracts covered by the [14], is acting for purposes other than his trade, business or profession. (As defined in [14].)

- **Customer**

A payer or a payee which may be either a consumer or a business.

- **Issuer**

A payment service provider providing the payment account and, in the context of this document, the mobile payment application to the customer

- **Mobile Equipment**

Mobile phone without UICC (also referred to as mobile handset)

- **Mobile Phone**

UICC + Mobile Equipment (also referred to as Mobile Station).

- **Mobile Contactless Payment**

A mobile phone initiated payment where the payer and payee (and/or his/her equipment) are in the same location and communicate directly with each other using contactless radio technologies, such as NFC (RFID), Bluetooth or infrared for data transfer (also known as proximity payments). In the context of this document all mobile contactless payments are mobile contactless card payments.

- **Mobile Remote Payment**

A mobile phone initiated payment where the transaction is conducted over telecommunication networks such as GSM or Internet, and can be made independently from the payer's location (and/or his/her equipment).

- **Payer**

A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order. ([14])

- **Payee**

A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction. ([14])

- **Payment Account**

Means an account held in the name of one or more payment service users which is used for the execution of payment transactions. ([14])

- **Payment Institution**

Legal person that has been granted authorisation in accordance with Article 10 of the [14] to provide and execute payment services throughout the Community. ([14])

- **Payment Transaction**

An act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee. (As defined in [14].)

- **Payment Service Provider**

The bodies referred to in Article 1(1) of the [14] and legal and natural persons benefiting from the waiver under Article 26 of the [14]. (As defined in [14].)

- **Payment System**

A funds transfer system with formal and standardised arrangements and common rules for the processing, clearing and/or settlement of payment transactions. (As defined in [14])

- **UICC**

Universal Integrated Circuit Card - A generic and well standardised secure element owned and provided by the MNOs.

- **Secure Element**

A tamper-resistant platform (device or component) capable of securely hosting applications and their confidential and cryptographic data (e.g. key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. Examples are UICC, embedded secure elements, chip cards, SD cards, etc..

Annex II – Abbreviations

Term	Definition
EDGE	Enhanced Data Rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
GPRS	General Packet Radio Services
ISO	International Organisation for Standardisation
MCP	Mobile Contactless Payment
NFC	Near-Field Communications
RFID	Radio Frequency Identity
SE	Secure Element
SIM	Subscriber Identity Module
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System

Table 9: Abbreviations

Annex III – Bibliography

Reference	Documentation
[1]	Arthur D. Little Global M-Payment Report Update - 2009
[2]	European Payment Council Customer-to-Bank Security Good Practices Guide http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=225
[3]	EMVCo http://www.emvco.com/
[4]	European Telecommunications Standards Institute http://www.etsi.org/
[5]	Global Platform http://www.globalplatform.org/
[6]	GSM Association http://www.gsmworld.com/
[7]	IDC Press release Jul 30th 2009 Smartphone Growth Encouraging, Yet the Worldwide Mobile Phone Market Still Expected To Shrink in 2009. http://idc.com/getdoc.jsp?containerId=prUS21950309
[8]	Internet Engineering Task Force http://www.ietf.org/
[9]	International Organisation for Standardisation http://www.iso.org
[10]	International Telecommunication Union World Telecommunication/ICT Indicators Database 2009 (13th Edition) http://www.itu.int/ITU-D/ict/publications/world/world.html
[11]	Mobey Forum http://www.mobeyforum.org/
[12]	Mobey Forum Alternatives for Banks to offer Secure Mobile Payments (version 1.0) http://www.mobeyforum.org/?page=white-paper-alternatives-for-banks
[13]	NFC Forum. 2009. http://www.nfc-forum.org/home.
[14]	Payment Services Directive Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market.
[15]	European Payments Council EPC 178-10 Mobile SEPA Contactless Implementation Guidelines (under preparation).
[16]	SD Card Association http://www.sdcard.org/developers/tech/smartsd/
[17]	European Payments Council EPC 20-08 SEPA Cards Standardisation (SCS) "Volume" - Book of Requirements http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=331

[18]	European Payments Council – GSM Association EPC 220-09 Mobile Contactless Payments Service Management Roles - Requirements and Specifications
[19]	European Telecommunications Standards Institute TS 102 221, TS 102 223, TS 102 22 and TS 102 226.
[20]	European Payments Council EPC 283-08 SEPA-e Payments Service Description (to be published)

Table 10: Bibliography

Annex IV – SEPA Payment Instruments

The Payment instruments promoted by EPC are:

- **SEPA Credit Transfer (SCT)**

The SCT Scheme enables payment service providers to offer a core and basic credit transfer service throughout SEPA, whether for single or bulk payments. The scheme's standards facilitate payment initiation, processing and reconciliation based on straight-through-processing. The scope is limited to payments in euro within SEPA countries, regardless of the currency of the underlying accounts. The credit institutions executing the credit transfer must be a Scheme participant; i.e. both must have formally adhered to the SEPA Credit Transfer Scheme. There is no limit on the amount of a payment carried out under the Scheme.

The SCT Scheme Rulebook [SCT] and the accompanying Implementation Guidelines are the definitive sources of information regarding the rules and obligations of the Scheme. In addition, a document entitled 'Shortcut to the SEPA Credit Transfer Scheme' is available which provides basic information on the characteristics and benefits of the SCT Scheme.

- **SEPA Direct Debit (SDD)**

The Core SDD Scheme - like any other direct debit scheme - is based on the following concept: "I request money from someone else, with their pre-approval, and credit it to myself".

The Core SDD Scheme [SDD] applies to transactions in euro. The debtor and creditor must each hold an account with a credit institution located within SEPA. The credit institutions executing the direct debit transaction must be scheme participants; that is, both must have formally adhered to the SDD Scheme. The Scheme may be used for single (one-off) or recurrent direct debit collections; the amounts are not limited.

- **SEPA Cards Framework (SCF)**

The SCF [SCF] developed by the EPC is a policy document which states how participants in the cards market such as card schemes, card-issuing banks, banks servicing card-accepting merchants and other service providers must adapt their current operations to comply with the SEPA vision for card payments in euro. While it is the choice of any participant in the cards market whether to become SCF-compliant or not, the EPC's members have pledged to conform to the conditions of the SCF in their capacities as issuers and acquirers.

Annex V – The Secure Element

A secure element is a certified tamper-resistant platform (device or integrated circuit component) capable of securely storing and executing applications and their confidential and cryptographic data (e.g. keys), in accordance to the rules and security requirements set forth by a set of well-identified trusted authorities. Secure elements are necessary for the storage and execution of mobile payment applications as dictated by the payment services institutions (the issuers).

Specific limitations introduced by the Mobile Phone form factor

Regardless of the final type of SE used, and in direct contrast to physical bank cards, specific provisions should be made to address the fact that, in most cases, payment service providers of the mobile payment application will not be in charge of deploying secure elements. The main reasons are:

- Only one, or at maximum, two, secure elements can be installed at any given time in a mobile phone. The user experience of swapping such devices from a mobile phone is very often impractical.

- The mobile phone itself is not typically deployed by the payment service providers and, contrary to the situation with bank cards, it is directly owned by the customer. Selection of mobile phones by customers is directly based on the features of the device (technical, esthetical, economical etc.), and not based on the requirements of the application providers. Therefore, an application provider attempting to deploy its own mobile phones will have no choice but to offer a wide selection of commonly available models from well-known handset manufacturers (similarly as all MNOs already do for their subsidised devices), incurring in unreasonable business costs.

- As any given user typically carries only "one" mobile phone; this phone must necessarily be shared between several application providers to allow for a competitive and fair market place for mobile services.

Identified Secure Elements Candidates for Mobile Payments

The Mobey Forum's document "Alternatives for Banks to Offer Secure Mobile Payments" provides an analysis of the current choices for Secure Elements [12]. It covers the following types:

- Stickers
  Contactless cards, manufactured in form of a sticker, which can be personalised and processed through the existing banking infrastructure. Customers can place the sticker on their phone for NFC payments.
- Secure Micro SD card
  Memory card products that hold an embedded chip which can be used as a secure element. These SD products may or may not hold a NFC antenna in addition.
- Universal Integrated Circuit Card (UICC)
  A generic and well standardised secure element owned and provided by the MNOs (see section 4.2.4).

- Embedded Secure Element
  A secure element embedded in a mobile phone at the time of its manufacture.
- Trusted Mobile Base
  Is a secure isolated section on the core processors (CPU) of mobile devices from various vendors into which various secure Applications can be provided

Although section 4.2.4.1 already includes specific challenges when then secure element is a UICC, it should be noted that each secure element type has also its own intrinsic challenges. Indeed, all secure element types share the following challenges to a varying degree:

- They may not be certified to the same security levels as those available for chip cards.
- If the supply chain infrastructure differs from that of payment chip cards, which will need to be re-certified to attain equivalent security levels;
- Payment chip cards are currently certified using a monolithic approach, the existing certification methods must be extended to allow for "arbitrary" on-the-field mobile contactless payment application installation.
- If shared between different service providers in different industries "firewall" must be built to separate the basic applications (issued by other service providers, such as ticketing) from the contactless card payment applications in each secure element. The same applies for contactless card payment application from different card issuers.
- Access to the secure element may be tightly controlled by the secure element issuer, therefore dedicated or mediated commercial relationships between each card issuers and each secure element issuers may be necessary.

For further reflections on the different types of secure elements, including challenges and opportunities, the reader is referred to the above mentioned Mobey Forum document.

End of Document