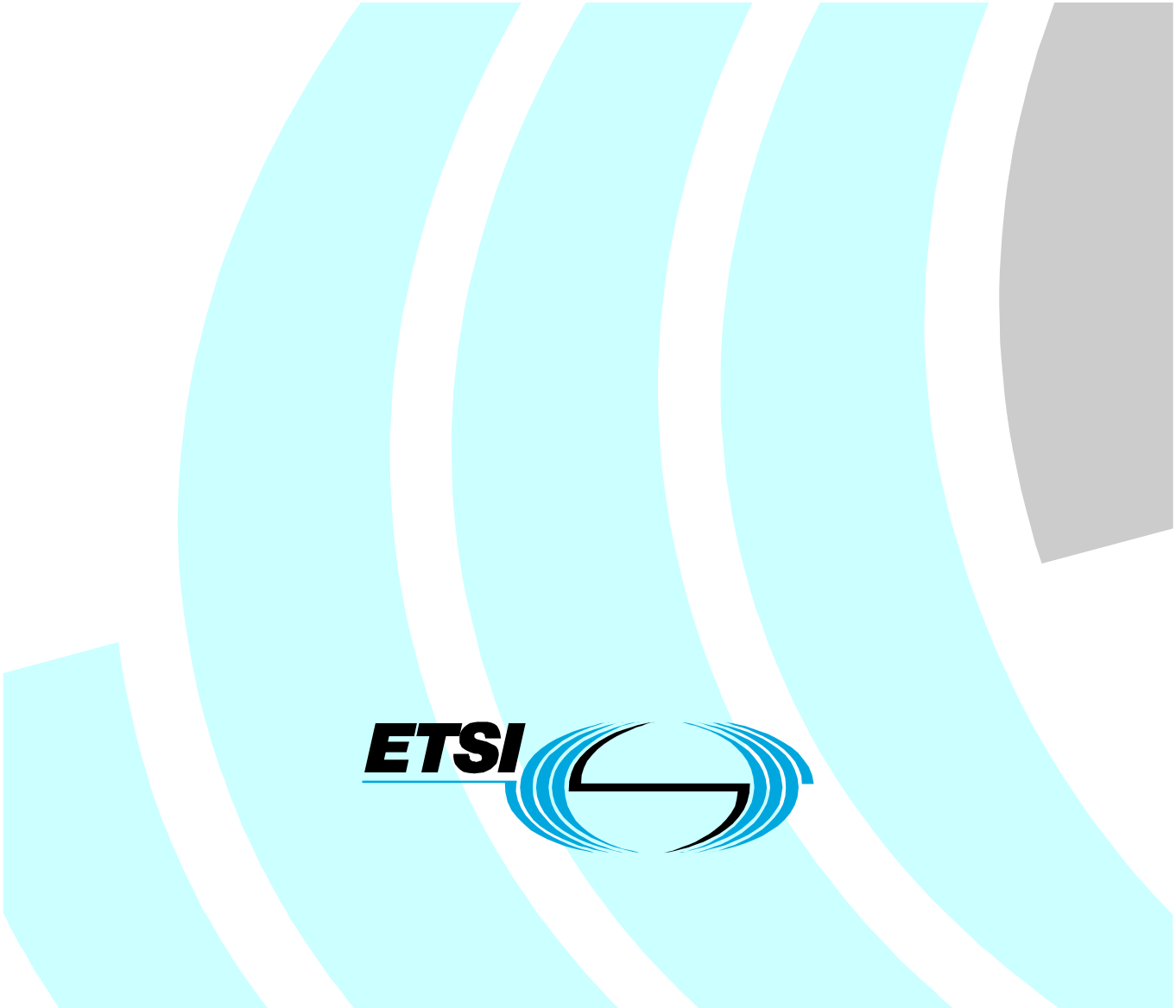
ETSI TR 102 071 V1.1.1 (2002-07)

Technical Report

Mobile Commerce (M-COMM); Requirements for Payment Methods for Mobile Commerce



Reference
DTR/M-COMM-02-003

Keywords
commerce, mobile, payment

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project M-Commerce (M-COMM).

1 Scope

The present document specifies the requirements which are necessary to be fulfilled by a telecommunications system in order to support a payment system in a mobile commerce environment.

2 References

For the purposes of this Technical Report (TR), the following references apply:

[1] ECBS ORG9003: "ECBS Terminology".

[2] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

3 Definitions

For the purposes of the present document, the following terms and definitions apply:

customer trusted environment: architecture consisting of a network and a set of hardware and software used by a customer to perform a transaction

mobile payment: payment as part of a commercial transaction between the customer and the service/goods provider or other customer

NOTE: The payment is effected through a mobile device. M-payments may be bank card-based or non-card-based, in both the real and virtual worlds.

mobile banking: range of traditional banking services, including push payments, where a customer gives an order to a bank to execute a transfer of funds, conducted via a mobile device

Mobile Commerce: electronic commerce using a mobile device as a customer device e.g. a mobile phone

mobile device: personal communication device (e.g. PDA, mobile phone etc) capable of communicating either locally (e.g. Bluetooth) or through a network (e.g. GSM)

payment enabler: provides infrastructure for generating an m-commerce transaction, but does not handle the transaction itself (e.g. a network operator or electronic wallet)**payment provider:** processor of m-commerce transactions

NOTE: A payment provider can be a bank, credit card institution, or other third party payment provider.

pull: schema where the client retrieves a document from a server by calling it (the destination of the information is the initiator of the communication)

pull payment (debit payment): The beneficiary initiates the request to transfer funds.

push: schema where the client receives a document without having explicitly asked for it (the originator of the information is the initiator of the communication)

push payment (credit payment): The customer (paying party) requests a funds transfer.

4 Payment systems in a mobile commerce environment

To fully understand how payments work in a mobile environment, this chapter describes a generic model and identifies the different actors and the systems involved in m-payments.

4.1 Generic model

The model in figure 4.1.1 illustrates the interactions between a customer, their mobile device, and a payment application. The merchant may be a physical merchant, trading on the high street, or a virtual merchant, trading via the Internet. The issue for the payment provider is how to assure their customers that they are engaging in "trusted" payments over open networks.

Clause 4.1.1 to 4.1.3 describe the stages of a possible m-payment transaction: the pre-payment dialogue, the payment dialogue and the post-payment dialogue. These three stages are necessary to complete a full transaction.

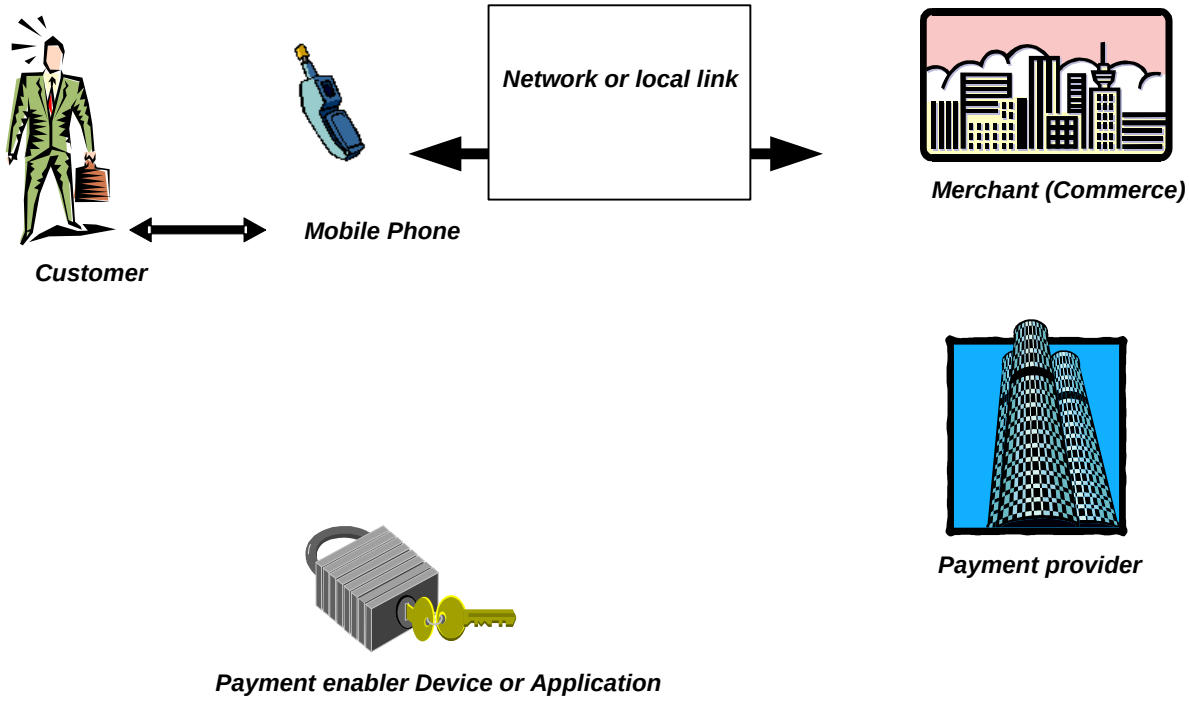


Figure 4.1.1: Generic model: Dialogue before payment

4.1.1 Dialogue before payment

The first step in a mobile payment transaction is when the customer communicates using the mobile device. The customer connects with the expected party (e.g. a service or content provider, a merchant, a public or private institution, etc.). Here security services (e.g. privacy, integrity or authentication services) may be required. Customer registration for a specific service might be required in order to verify personal data.

4.1.2 Payment dialogue

In the second step, the customer selects the goods/contents/service to be purchased. The customer and the expected party (e.g. a service or content provider, a merchant, a public or private institution, etc.) may agree on a contract related to the goods/contents/service to be purchased (mutual confirmation of goods to be purchased).

Then the customer communicates via the mobile device to the payment enabler. The customer selects the means of payment (brand, type of payment, etc.) and communicates with the payment provider. At this stage, the payment provider and the customer need to be assured that they are communicating securely. The security needs to be appropriate to the transaction. The customer will need to have to an appropriate perception of security to be reassured to use the system. The payment is initiated and the parties are informed whether the payment has been terminated (authorized or rejected), with identification if appropriate.

4.1.3 Processing after payment

In the final stage, the payment provider processes the payment within the financial institutions (i.e. merchant acquirer) as it is done today.

4.2 Requirements of a payment system

4.2.1 Confidentiality

4.2.1.1 Definition

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

ECSB ORG9003 [1], ISO 7498-2 [2].

4.2.1.2 Requirements

The following information shall be confidential:

- Payment card identification.
- PINs.
- Identity of user (and his contact information).

NOTE: This list is not exhaustive, and may include the content, the shopping experience, delivery information.

In certain cases the confidentially content may be required, for example:

- Content covered by copyright.

4.2.2 Authentication

4.2.2.1 Definition

The term is used in different contexts:

Authentication: Process used between a sender and a receiver to provide data origin verification , see [1].

Data origin authentication: corroboration that the source of data received is as claimed, see [1].

NOTE 1: The source of data may be the user or a device.

NOTE 2: The cardholder authentication process can be made combining the information on the message originator (e.g. the CLI) and verification of a defined quantity (e.g. a PIN, the answer to a challenge, biometrics). known only by the cardholder himself.

NOTE 3: In each transaction, the user is authenticated, and also his intention to initiate the transaction.

4.2.2.2 Requirements

In each transaction, it shall be possible to authenticate the user and the transmitted data. The degree of accuracy shall be as good as non-mobile transactions. The system shall provide proof of authentication for each transaction to the payment provider.

NOTE: Authentication at the beginning of a session (e.g. at power on) may be sufficient for some types of transactions.

4.2.3 Integrity

4.2.3.1 Definition

The property of ensuring that information is not altered in any way, either by accident or with fraudulent intent, see [1].

NOTE: Any alteration shall be detectable on the receiver side.

4.2.3.2 Requirements

The transmission system shall provide a mechanism for data integrity, and shall be able to demonstrate the integrity of each transaction and of stored data.

Integrity requirements apply both to the information provided to the payment provider and to the information provided to the user.

EXAMPLE: The amount of a transaction seen on a user screen needs to be the same as the amount contained in the transaction.

4.2.4 Non repudiation

4.2.4.1 Definition

Non-repudiation: a process that involves delivering data in such a way that the receiver can not deny receipt and the sender can not deny sending it, see [1].

non-repudiation of origin: the property that the originator of a message is not able to subsequently deny, with an accepted level of credibility (defined either in legislation or in a contract between the customer and the payment provider), having originated the message.

non-repudiation of receipt: the property that the receiver of a message is not able to subsequently deny, with an accepted level of credibility (defined in a contract between the customer and the service provider), having received the message.

NOTE: This assumes the integrity of the original message.

4.2.4.2 Requirements

A transaction which has been properly authenticated, it shall be considered to be non-repudiable. The payment provider shall receive a report sufficient to demonstrate the non-repudiability of each transaction.

EXAMPLE: A signature given by the payment device, indicating that the card was present and the PIN was entered, to the merchant may fulfil this requirement.

4.2.5 PIN entry

4.2.5.1 Definition

Personal Identification Number (PIN): A code or password the customer possesses for verification of identity, see [1].

PIN Entry Device (PED): Any device into which the cardholder inputs the PIN. A PED may also be called a PIN pad, see [1].

4.2.5.2 Requirements

It shall be possible for the user to modify his PIN.

4.2.6 Secure mode indication

4.2.6.1 Definition

An indication to the user that he is operating in a protected environment when entering sensitive data (e.g. PIN).

4.2.6.2 Requirement

Payment applications shall provide an indication of security at the user interface.

NOTE: Security requirement is that the mobile has to provide some form of secured access between payment application and display and keyboard, in order to prevent some possibility of frauds like capture of the PIN through the network or display a different amount from what is sent to the payment provider. This secured access mode has to be shown to the user through some unambiguous indication on the mobile via for example display, led, etc.

5 Scenarios for a mobile payment system

5.1 Dual SIM/dual slot

In this scenario, the mobile device is provided with two physical SIM cards: one identifying the customer to the telecommunications operator; the second as a payment card to the payment provider.

5.1.1 Confidentiality in a dual SIM system

May be provided through the SIM/WIM chip (WTLS on the OTA link) and relevant SSL protocol between WAP Gateway and payment provider server or through a process at application level involving the payment card/chip.

5.1.2 Authentication in a dual SIM system

Payment data signature is provided through the payment enabler card/chip, etc.

5.2 Single SIM

In this scenario, the mobile device is provided with a single SIM card, which acts as a SIM for the telecommunications operator and as a payment card for the bank.

SIM operating system will be in the near future a multi-application OS, e.g. JAVA 2.1 based. It has to be trusted by payment providers in concerns like secure loading/downloading of applications, isolation between private data of these application, etc.

5.2.1 Confidentiality in a singleSIM system

May be provided through the SIM/WIM chip (WTLS on the OTA link) and relevant SSL protocol between WAP Gateway and payment provider server) or through a process at application layer involving the payment application in the SIM.

5.2.2 Authentication in a single SIM system

Payment data signature is provided through the payment enabler application inside the SIM.

5.3 Small payment/electronic wallet (proxy payment)

Two scenarios may be mentioned:

- In first scenario, the mobile device is loaded with pre-authorized funds. At the time a transaction is made no link is made to a network.
- In second scenario, a customer account, located somewhere in the network, is loaded with pre-authorized funds. At the time of the transaction, a link to the network is required. For example, this second approach is more relevant for µ-payment of contents obtained though the network.

Annex A:
Examples of possible mobile payment scenarios

A.1 Example of an m-payment using 3D model

In the next model, the interactions between the system and the actors and the flow of a typical mobile commerce transaction are described.

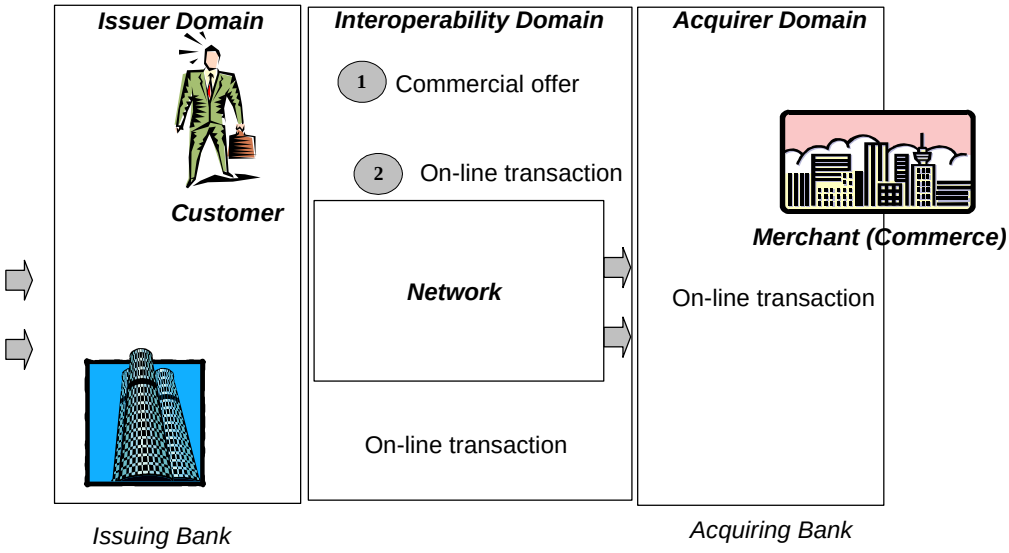


Figure A.1: 3D Model showing interactions between the systems and actors

In the payment schemes, this model is referred to as the 3D (Three Domain) model. It looks at the activity between the following parties: the merchant and their bank - Acquirer Domain, the cardholder and their bank - Issuer Domain, and the cardholder's bank and the merchant's bank - Interoperability Domain. The fundamental role of each of the actors, however, is similar to the traditional roles played by each one. The diagram overleaf shows the flow of a mobile payment. The flow of the transaction can be clockwise or anti-clockwise, i.e., an acquirer-centric model or an issuer-centric model. *On some occasions*, part of the transaction links the customer directly to the acquiring bank. With the implementation of EMV, a direct link between the issuing bank and the merchant may also be feasible. This 3D model fully applies to the m-commerce environment.

The different steps involved in the process of the transaction in the model are described below.

1) **Commercial Offer** (pre-payment dialogue) - The customer agrees on the product or service he wants to buy. This may be the legally binding phase for the purchase but does not concern the payment transaction process, and should be differentiated in all business, legal, marketing and technical aspects

2) Once the previous phase is completed, the actual **transaction phase (payment dialogue)** may proceed. The customer normally initiates this phase by expressing his willingness to pay. The transaction proposition is linked in some way (common data) to the commercial offer.

   In an online transaction (the most frequent in a mobile environment), the customer asks for an acceptance request of the transaction. The transaction has to be authorized by the issuing or accepting bank. In order to authorize the transaction the Issuing bank needs to authenticate the customer (make sure that the customer is the individual he claims to be) through a challenge request. If the customer answer is compliant with the challenge itself then he/she is authenticated and the transaction is processed.

   Once the transaction is authorized, the merchant may deliver the service or product to the customer.

   The first two phases are normally real time. The third is not usually real time.

3) Settlement (post-payment dialogue) is then performed (offline or online) to debit the customer's account and to credit the merchant's account.

   During the process, transaction data may need to be signed to assure the concerned party that the operation has been performed correctly by the right entity.

   In this generic transaction model, data may flow through different networks. However, what is common to all scenarios in a mobile environment, is that the *consumer trusted payment system* communicates via Over The Air (OTA) channels (SMS, WAP, etc.).

   A number of transaction protocols already exist (e.g. SET, 3D Secure, SSL). These protocols and their implementation are evolving fast and this may lead to new banking requirements for security.

A.2 Example of an M-Payment via Payment Provider

This model describes the payment process with payment provider in 5 steps:

1) Customer and Merchant negotiate and agree on the conditions of their commercial relationship (product, delivery, conditions of payment, payment provider, etc.).

2) The merchant sends a payment request to the payment provider including the transaction data.

3) The payment provider triggers a signature/confirmation request containing the transaction data to the mobile customer via network operator.

4) The customer signs/confirms the transaction data and sends the signature/confirmation back to the payment provider. The payment provider or the payment enabler (e.g. the network operator on behalf of the payment provider) is able to verify and authenticate the customer's response.

5) There might exist two different relationships between payment provider and merchant/bank:

   a) The payment provider debits the customer's account (direct debit), credits the merchant's account and confirms the merchant that the transaction is executed.

   b) If the payment is based on a credit card, the Payment provider request a transaction authorization to the Issuing Bank via the payment scheme network. The Issuing Bank authorizes the transaction and debits the customer account. The payment provider confirms the merchant that the transaction is executed and the merchant's acquirer credits the merchant account.

Relationship exists between:

- Customer and Payment Provider.
- Customer and Network Operator.
- Network Operator and Payment Provider.
- Payment Provider and Merchant.
- Payment Provider and Bank.

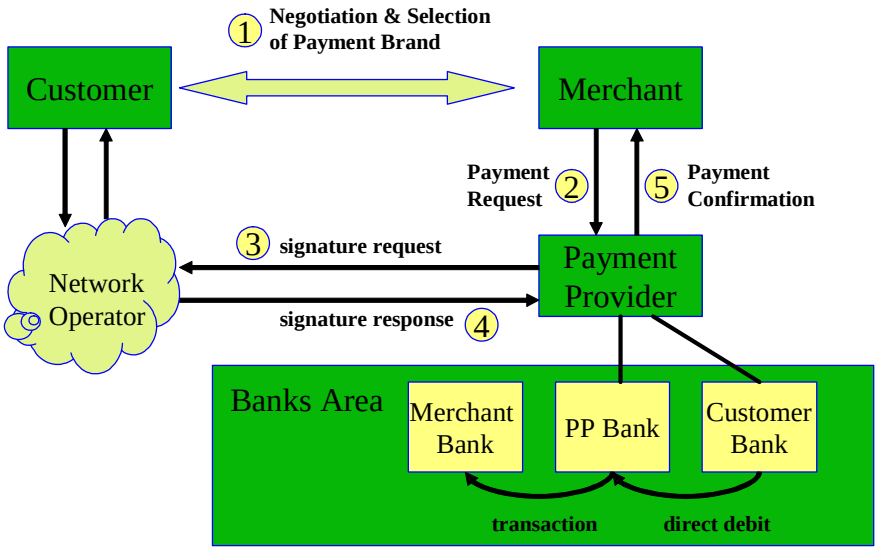

1
Negotiation & Selection
of Payment Brand
Customer
Merchant
Payment
Request
2
5
Payment
Confirmation
3
signature request
Network
Operator
Payment
Provider
signature response
4
Banks Area
Merchant
Bank
PP Bank
Customer
Bank
transaction
direct debit

Figure A.2

Annex B: Bibliography

- draft ECBS DTR 603: " Draft Business and Functional Requirements for Mobile Payments".

History

Document history		
V1.1.1	July 2002	Publication