



EUROPEAN CENTRAL BANK

EUROSYSTEM

OVERSIGHT FRAMEWORK FOR CARD PAYMENT SCHEMES – STANDARDS

JANUARY 2008

ECB EZB EKT EKP





EUROPEAN CENTRAL BANK

EUROSYSTEM



OVERSIGHT FRAMEWORK FOR CARD PAYMENT SCHEMES- STANDARDS

JANUARY 2008

In 2008 all ECB
publications
feature a motif
taken from the
€10 banknote.

© European Central Bank, 2008

Address

Kaiserstrasse 29
60311 Frankfurt am Main
Germany

Postal address

Postfach 16 03 19
60066 Frankfurt am Main
Germany

Telephone

+49 69 1344 0

Website

<http://www.ecb.europa.eu>

Fax

+49 69 1344 6000

All rights reserved. Reproduction for educational and non-commercial purposes is permitted provided that the source is acknowledged.

Unless otherwise stated, this document uses data available as at 11 May 2007.

ISBN 978-92-899-0214-4 (online)



CONTENTS

1 BACKGROUND	5
2 CHARACTERISTICS OF THE FRAMEWORK	5
3 SCOPE OF THE FRAMEWORK	6
4 ADDRESSEE OF THE FRAMEWORK	6
5 WAIVER POLICY	6
6 METHODOLOGY	6
6.1 Risk profiles	7
6.2. Definition of risk profiles	7
7 THE OVERSIGHT STANDARDS	8
1 The CPS should have a sound legal basis under all relevant jurisdictions	9
2 The CPS should ensure that comprehensive information, including appropriate information on financial risks, is available to the actors	10
3 The CPS should ensure an adequate degree of security, operational reliability and business continuity	11
4 The CPS should have effective, accountable and transparent governance arrangements	15
5 The CPS should manage and contain financial risks in relation to the clearing and settlement process	16
ANNEXES	
Overview of card payment schemes	17
Glossary of terms	19



I BACKGROUND

In many European countries, payments by card represent the vast majority of cross-border retail transactions and are the most common means of effecting payments over the Internet. Statistics for the euro area show that, in the past five years, the use of both debit and credit cards has almost doubled. The euro area is home to more than twenty card schemes, but the market is still fragmented, since the majority of card schemes consist of national debit card schemes. The increasing use of cards makes card security and infrastructure of concern to both central banks and the market.

Under Article 105(2) of the Treaty establishing the European Community and Articles 3 and 22 of the Statute of the European System of Central Banks and of the European Central Bank (ECB), one of the basic tasks of the Eurosystem is to promote the smooth operation of payment systems. In this context, the ECB's policy statement¹ in 2000 clarified the role of the Eurosystem in the field of payment systems oversight. In particular, it states that "The Eurosystem may also formulate policy concerning the security of payment instruments in order to maintain the confidence of the users of the payment systems."

Pursuant to this mandate, the Eurosystem decided to develop a common oversight policy in order to promote the reliability of *card payment schemes (CPSs)* operating in the euro area, public confidence in card payments and a level playing field across the euro area in a unified market. The oversight framework for CPSs is based on a "building block" and risk-based approach to ensure, in particular, that it is built on a sound knowledge of the functioning of the market for card payments and properly addresses the relevant risks to which card schemes are exposed. This document is structured as follows. Section 2 recalls the main characteristics of the framework governing the implementation of the oversight standards. Sections 3 and 4 present the scope and addressee of the framework, respectively. Section 5 outlines the waiver

policy and Section 6 explains the methodology. Section 7 elaborates on the possible content of the standards. In addition, a model represents how CPSs work in Annex I and a glossary is provided in Annex II. The terms included in the glossary appear in italics in the document.

2 CHARACTERISTICS OF THE FRAMEWORK

The majority of European Union central banks already have an ad hoc oversight policy for CPSs. Almost all central banks directly oversee CPSs as far as security issues are concerned, with the objective of maintaining public confidence in means of payment and thus ultimately in money. Over three-quarters of European central banks consider the efficiency of CPSs to form part of their responsibilities. However, the central banks do not follow common standards or evaluation guidelines. CPSs are assessed against a variety of standards, such as the "Core Principles for Systemically Important Payment Systems"², best industry practices in security management and other areas, or against a risk-based approach. With regard to the gathering of information on card schemes, the vast majority of central banks collect statistical data and general information from CPSs or issuers and, in some cases, information on international card payment schemes is exchanged among overseers.

From this perspective, the aim of the present analysis is to establish a minimum set of oversight standards for CPSs based on the experience gained so far. The rationale behind these standards is largely the same as that governing the oversight standards for euro retail payment systems³, but also accommodates the needs of CPSs in terms of safety and efficiency. These oversight standards are independent of any legal or professional rules applicable to CPSs.

1 "Role of the Eurosystem in the field of payment systems oversight", ECB, Frankfurt, June 2000.

2 "Core Principles for Systemically Important Payment Systems" (also referred to as the "Core Principles Report"), Bank for International Settlements (www.bis.org), Basel, January 2001.

3 "Oversight standards for euro retail payment systems" ECB, Frankfurt, June 2003

3 SCOPE OF THE FRAMEWORK

The framework shall apply to all card payment schemes, including three-party and four-party CPSs providing card payment services either by debit and/or credit card. A definition of a CPS is provided in Box A. Cards debiting prepaid and dedicated accounts, are covered by the CPS oversight framework. However, prepaid cards, where the electronic value is directly stored on the card, are beyond its scope, as they fall under the Eurosystem oversight framework for e-money.

4 ADDRESSEE OF THE FRAMEWORK

In principle, the standards of the framework are addressed to the *Governance Authority*, which is responsible for ensuring compliance. However, in agreement with the overseer, the Governance Authority may appoint other specific actor(s) to be responsible for certain CPS functions. In such cases, the boundaries for responsibility of these actors must be clearly defined, transparent and documented.

5 WAIVER POLICY

In order not to stifle innovation, overburden small CPSs and allocate oversight efforts proportionately to the risks created by the schemes, a waiver policy shall apply. This waiver has been defined taking into consideration the European dimension

of CPSs in the context of the future Single Euro Payments Area (SEPA), the cross-border use of cards today, the impact that the malfunction of a CPS would have on the confidence of the public in cards and the risks which would materialise in the form of loss of money.

A CPS may be excluded from the application of the oversight standards if it satisfies the following criteria within the euro area:

- a. over the past three years, the sum of cards in-issue is on average less than 1 million per year; or
- b. over the past three years, the CPS has an annual average value of transactions of less than €1 billion.

National central banks (NCBs) may decide to apply stricter rules on CPSs under their jurisdiction that are entitled to a waiver on the basis of risk considerations and the relative importance of the CPS in the national context.

6 METHODOLOGY

The oversight standards have been developed on the basis of risk profiles (see below). The oversight standards for euro retail payment systems are a logical model for the standards, but they have been adapted to the specificities of CPSs, especially with regard to security and operational issues. The key issues relating to

Box

CARD PAYMENT SCHEME (CPS) – A DEFINITION

For the purposes of this framework, a card payment scheme is the set of functions (see Annex 1), procedures, arrangements, rules and devices that enable a holder of a *payment card* to effect a payment and/or cash withdrawal transaction with a third party other than the card issuer. The oversight framework covers the entire payment cycle, i.e. the *transaction phase* (including the manufacture of payment instruments and the processing of data) and the clearing and settlement phase. It accommodates concerns relating to both the retail payment system and the payment instrument used.

each standard are explored and explained in an explanatory memorandum that focuses on the specificities of CPSs.

6.1 RISK PROFILES

A risk analysis was carried out to identify assets that need to be protected in order to safeguard the smooth functioning of CPSs. These assets are exposed to different risk profiles. Risks may emerge directly (e.g. card counterfeiting) or be derived from other risks (loss of reputation as a result of card counterfeiting), and not all of these risks carry the same weight. However, due attention should be paid to each of these risks, as they may have a direct or indirect impact on the safety and efficiency of a CPS.

There are risks of a legal, operational and financial nature in every payment system. The significance of these risks and their impact on the smooth functioning of a payment system depend on the nature of the system. For example, in the case of systemically important payment systems, the materialisation of financial risks may cause serious disruption to financial stability, while in retail payment systems, they might not have the same impact. To a greater or lesser degree, these risks are also apparent in CPSs. While their materialisation may not lead to the kinds of systemic financial disruption encountered in the case of systemically important payment systems, they may nevertheless have what is known as a system-wide impact, i.e. they could disrupt, at least temporarily, the functioning of the real economy by severely altering the capacity of economic agents to discharge their obligations on account of the unavailability of and/or lack of confidence in payment cards and substitutable payment instruments. Of course, in practice, the severity of the impact will be dependent on the market structure for payment services and, in particular, on the importance of cards and other substitutable payment instruments.

CPSs should be protected against risks that arise throughout the entire payment cycle, not only in the clearing and settlement phase, meaning that it is particularly important to put in place

efficient and effective governance arrangements. Inefficient governance arrangements could fuel all other types of risk, while governance issues cannot always be addressed via measures for other types of risk (e.g. operational risk). To deal with the risk of poor governance arrangements, an “Overall management” risk profile has been introduced.

Furthermore, owing to the nature of CPSs, the risk of loss of reputation is greater than for other types of payment systems. Breach of reputation can have a severe impact on confidence in cards, justifying the identification of a “Reputational” risk profile. More commonly, reputational risk arises as a result of other risks (e.g. legal and operational), but the possibility of the direct materialisation of reputational risk cannot be ruled out (e.g. dissemination of false information).

The CPS oversight standards have a strong focus on operational risk for two reasons. First, the mitigation of operational risk is key to the smooth functioning of a CPS. Inadequate security, operational reliability or business continuity of a CPS may result in a loss of public confidence in cards and, in turn, market disruption. Second, the management of operational risk should take into account the specificities, variety and complexity of CPSs, especially with regard to technical aspects and outsourcing, which requires a deep insight into the CPS infrastructure.

6.2. DEFINITION OF RISK PROFILES

Legal risk refers to the risk of loss as a result of the unexpected application of a law or regulation, or because a contract cannot be enforced. Legal risk may arise if the rights and obligations of parties involved in the CPS are subject to legal uncertainty. The analysis of legal risks in a card scheme is difficult owing to the complexity and diversity of CPSs, which involve various steps and stakeholders (e.g. operators, *issuers*, *acquirers*, *cardholders* and *card acceptors*). The legal structure of card schemes operating internationally is even more complex, as a

variety of regulatory frameworks have to be considered in order to ensure enforceability under all relevant jurisdictions.

Financial risk covers a range of risks incurred in financial transactions, including both liquidity and credit risk. The oversight standards also aim at mitigating financial risks to CPSs, including potential losses resulting from operational risks (e.g. fraud). The clearing and settlement phase of card schemes may give rise to financial risks related to the default or the insolvency of the settlement agent or *service providers*. In particular, the acquirer may face liquidity or credit risk if the issuer is not able to settle an obligation.

Overall management risk generally refers to a lack of policies for adequate governance and management of CPSs. An overall management risk usually arises if roles and responsibilities are not properly assigned and if decisions regarding objectives and performances are not shared by all actors. An overall management risk often originates other risks (operational, legal, etc.), since it relates to the core governing functions of any CPS. The main consequences of such a risk are a potential conflict of interest among actors and the inability or unwillingness to sustain market dynamics and innovations and react appropriately to crises. This risk may also have a competitive impact if access policies are non-transparent and inappropriate. In the event of crises, the lack of a proper definition of roles and responsibilities can hamper a prompt reaction on the part of the CPS.

Operational risk results from inadequate or failed internal processes and systems, and from human error or external events related to any element of the CPS. Operational risk can arise as a result of a failure to follow or complete one or more steps in the payment process. Operational risk includes the risk of fraud, since this can be defined as a wrongful or criminal deception, which may lead to a financial loss for one of the parties involved and may reflect inadequate safety arrangements. A typical fraud risk is the unauthorised debit of a cardholder account.

Reputational risk can be defined as the potential for negative publicity regarding an institution's business practices – whether or not grounded in fact – to cause a decline in the customer base, costly litigation, revenue reductions, liquidity constraints or a significant depreciation in market capitalisation. Since customers tend to choose a CPS for its reputation and cost, reputational risk is very important. Reputational risk relates mainly to brand management. What makes reputational risk difficult to quantify and/or identify is that it is both a risk in itself and a derivative risk, i.e. one which stems from other areas of risk and vulnerability. A breach of reputation may be the unexpected outcome of operational problems or of the provision of erroneous or insufficient information to end-users. In other words, as with bank runs, reputational risk generally results from vulnerabilities in other risk areas; however, once it has started, it has its own relevance and requires specific action.

7 THE OVERSIGHT STANDARDS

On the basis of the above, and taking into account the matrix in Appendix 1, five standards have been identified: legal issues, transparency, operational reliability, good governance and sound clearing and settlement processes. In short, each CPS should:

1. have a sound legal basis under all relevant jurisdictions;
2. ensure that comprehensive information, including appropriate information on financial risks, is available to all actors;
3. ensure an adequate degree of security, operational reliability and business continuity;
4. implement effective, accountable and transparent governance arrangements; and
5. manage and contain financial risks in relation to the clearing and settlement process.

STANDARD I: THE CPS SHOULD HAVE A SOUND LEGAL BASIS UNDER ALL RELEVANT JURISDICTIONS

KEY ISSUES

1.1 The legal framework governing the establishment and functioning of a CPS and the relationship between the CPS and its issuers, acquirers, *customers* and service providers should be complete, unambiguous, up-to-date, enforceable and compliant with the applicable legislation.

1.2 Where different jurisdictions govern the operation of the CPS, the law of those jurisdictions should be analysed in order to identify the existence of any conflict. Where such conflict exists, appropriate arrangements should be made to mitigate the consequences of such conflict.

EXPLANATORY MEMORANDUM

- The absence of a correct legal incorporation could lead to the unlawfulness of all rules and contractual arrangements governing the CPS and its relations with its *actors*.

Where the rules and/or contractual arrangements do not comply with the applicable legislation, they (or certain parts thereof) will be invalid, which may give rise to uncertainties. It is therefore important to pay due attention to legal compliance from the outset. It is during the establishment phase that the foundations are laid for the sound functioning of the scheme in the future.

Where the legal framework of the CPS is sound, and its rules and contractual arrangements are unambiguous, all of its actors will have a clear understanding of their rights and obligations. This minimises the possibility of their being confronted with unexpected risks and costs resulting from ambiguous legal formulations.

As the law can change, the absence of regular monitoring of the legal environment and prompt adaptation of CPS rules and contracts could create conflicts between the CPS rules

and current legislation and lead to uncertainty regarding the CPS. For example, a CPS may face the risk of scrutiny by competition or data protection authorities given the nature of its business. Crystallisation of such risk could ultimately have serious consequences for the CPS concerned.

- A CPS may operate in a cross-border environment. Such an environment complicates the task of ensuring legal certainty. Furthermore, in this context, it is very important that the rules and contractual arrangements clearly and unambiguously specify the governing law and the relevant jurisdiction. If these are not specified, the enforceability of the CPS rules and contractual arrangements may be challenged in the event of a dispute.

STANDARD 2: THE CPS SHOULD ENSURE THAT COMPREHENSIVE INFORMATION, INCLUDING APPROPRIATE INFORMATION ON FINANCIAL RISKS, IS AVAILABLE TO THE ACTORS

KEY ISSUES

2.1 All rules and contractual arrangements governing the CPS should be adequately documented and kept up to date. All actors and potential actors should be able to easily access information relevant to them, to the extent permitted by data protection legislation, so that they can take appropriate action in all circumstances. Sensitive information should only be disclosed on a need-to-know basis.

2.2 Issuers, acquirers, cardholders and card acceptors should have access to relevant information in order to evaluate financial risks affecting them.

CPSs, they may not be in a position to identify and assess the risks that could affect them.

EXPLANATORY MEMORANDUM

- In the absence of proper documentation (e.g. contracts) regarding the roles and responsibilities of all actors involved in a CPS or of a proper management of communication between these actors, an overall management risk could arise. In a CPS this is especially true, since the operational risk, including fraud, could lead to financial losses for one or more of the parties involved. For example, lack of consistent and up-to-date information on how to mitigate fraud – e.g. information on recognising skimming devices and protecting PINs – may cause financial loss and decrease confidence in the payment instrument. However the disclosure of sensitive information could endanger the security of the CPS.

Relevant documentation for evaluating possible risks stemming from participation in the CPS should also be available to potential actors.

- If issuers, acquirers, cardholders and card acceptors do not have access to information about the risks they face as a consequence of participating in a scheme, they may face potential risks stemming from clearing and settlement, and from fraud and/or chargeback obligations. Owing to the complexity of

STANDARD 3: THE CPS SHOULD ENSURE AN ADEQUATE DEGREE OF SECURITY, OPERATIONAL RELIABILITY AND BUSINESS CONTINUITY

3 KEY ISSUES

3.1 *Security management*

3.1.1 An analysis of operational and security risks should be conducted on a regular basis in order to determine the acceptable risk level and select adequate security policies and appropriate procedures in order to prevent, detect, contain and correct security violations. Compliance with such security policies should be assessed on a regular basis.

3.1.2 Management and staff should be trustworthy and fully competent (in terms of skills, training and number of staff) to make appropriate decisions to endorse security policies and carry out their CPS-related responsibilities and duties.

3.1.3 Operational and incident management should be clearly defined and effectively implemented.

3.1.4 The CPS security policy should ensure privacy, *integrity* and *authenticity* of data and *confidentiality* of secrets (e.g. *PIN*) when data are operated, stored and exchanged. If secrets are revealed or compromised, effective contingency plans should be implemented to protect the CPS.

3.2 *Manufacture and distribution of cards*

3.2.1 The design and manufacture of payment cards and of accepting and other technical devices should ensure an adequate degree of security in line with the security policies of the CPS.

3.2.2 Effective and secure procedures should be in place for the initialisation, personalisation and delivery of both cards to holders and *accepting devices* to acceptors, and for the generation and delivery of secrets (e.g. *PIN*).

3.3 *Transactions*

3.3.1 Adequate security standards should be in force for the initiation of transactions in accordance with CPS security policies. CPS components should be protected from unauthorised activity. The CPS should have the capability to mitigate the risks stemming from the use of payment cards without online authorisation or with less secure *authentication* measures (e.g. remote payments).

3.3.2 The activities of cardholders and card acceptors should be permanently monitored in order to enable a timely reaction to fraud and any risks posed by such activities. Appropriate measures should be in place to limit the impact of fraud.

3.3.3 Appropriate arrangements should be made to ensure that card transactions can be processed even at peak times and on peak days.

3.3.4 Sufficient evidence should be provided to enable a transparent and easy clarification of disputes between actors.

3.4 *Clearing and settlement*

3.4.1 Clearing and settlement arrangements should ensure an adequate degree of security, operational reliability and availability, taking into account the settlement deadlines specified by the CPS.

3.5 *Business continuity*

3.5.1 Business impact analyses should clearly identify the components that are crucial to the smooth functioning of the CPS. Effective and comprehensive contingency plans should be in place in the event of a disaster or any incident that jeopardises CPS availability. The adequacy and efficiency of such plans should be tested and reviewed regularly.



3.6 Outsourcing

3.6.1 Specific risks resulting from *outsourcing* should be managed explicitly and appropriately through comprehensive and appropriate contractual provisions. These provisions should cover all relevant issues, for which the actor who outsources activities within the CPS is responsible.

3.6.2 Outsourcing partners should be appropriately managed and monitored. Actors who outsource activities should be able to provide evidence that their outsourcing partners comply with the standards for which the actor itself is responsible within the CPS.

EXPLANATORY MEMORANDUM

Operational risks, including fraud, could have a serious impact on the CPS and endanger its financial stability, leading to a financial loss for one or more of the parties involved. It could also undermine users' confidence in the CPS. Mitigation of these risks supposes appropriate measures to ensure:

- proper security management;
- protection of sensitive data or devices during manufacturing and distribution of cards;
- secure initiation and operation of transactions;
- secure and reliable clearing and settlement;
- business continuity; and
- control of outsourcing.
- **Proper security management**
 - If the CPS does not conduct regular analyses of operational and security risks using widely accepted and up-to-date methodologies, it may not be able to define appropriate and comprehensive security policies for the scheme. A lack of

proper risk management could result in the existence of a set of security standards that do not minimise or eliminate security risks at an acceptable cost. If risk management does not demonstrate clear support for and commitment to the implementation of the security policy, risks may not be adequately addressed.

- If staff are inadequately qualified or the number of staff insufficient to cope with the security challenges involved, this may hamper the smooth functioning of the CPS. Insufficient knowledge on the part of management regarding risk management processes and IT security-related aspects may lead to inappropriate decisions being made.
- Security incidents can happen even when all precautions appear to have been taken. It may be impossible to detect the origin of incidents or to identify the type of vulnerability present. This could be attributable to inadequate or missing contingency plans for limiting the damage. Moreover, if a clear and comprehensive understanding and definition of the assets does not exist, it will be difficult to identify the impact of a security breach. Security incidents also arise as a result of failure to transmit alerts to the relevant recipients, as a consequence of which they will be unable to properly react to vulnerability and fraud.
- Theft, counterfeit, malfunctioning, destruction, alteration, entrapment and/or illicit use of CPS components may have serious consequences for the secure functioning of the scheme in terms of confidentiality, integrity and availability. Such attacks can jeopardise software, hardware or data relevant to the proper functioning of the CPS (e.g. secrets, technical parameters and transaction attributes). These problems could occur, in particular, when the design and manufacture of CPS components do not rely on uniformly adequate, up-to-date

security standards and when they are not regulated by an approval procedure based on rules defined by the CPS governance authority. Moreover, the availability and functioning of the CPS could be affected by other applications, payment schemes or CPSs. This could happen, for example, where several kinds of application are embedded in a given CPS component or there is no strict separation (in terms of both logical design and technical security features). Secrets (e.g. *PIN*) could be disclosed or compromised and used to copy components in order to make fraudulent payments if they are not properly managed and their confidentiality is not well protected.

- **Protection of sensitive data or devices during manufacturing and distribution of cards, accepting and other devices**

- A clear and comprehensive view of the specific security standards for the design and manufacturing of cards, accepting and other devices is important to combat fraud and misappropriation of sensitive data. It is important that security standards are based on and comply with the CPS security policy, otherwise incorrect or inappropriate security measures could be implemented.
- Personal information, secrets (e.g. *PIN*), cards or data representing a card could be stolen (e.g. card numbers intercepted on the Internet) or compromised and used for fraudulent payments if the initialisation or personalisation of CPS components is inadequate or missing. If delivery of both cards to holders and *accepting devices* to acceptors is inappropriately protected against theft or misappropriation, there is a risk of fraud.

- **Secure initiation and operation of transactions**

- If security measures like *authentication* methods are inadequate or missing,

transactions could easily be initiated fraudulently. This could happen when personal information, secrets (e.g. *PIN*), cards or data representing a card are stolen (e.g. card numbers intercepted on the Internet) or compromised. Stolen information can also be used to create fake documents, open bank accounts or obtain other payment cards. If unauthorised persons are able to execute actions, risks to the confidentiality, privacy, availability and integrity of data or secrets can arise. Moreover, risks resulting from deliberate actions or unintentionally incorrect behaviour can arise if unauthorised intrusions to premises requiring protection (e.g. premises where secrets are stored) or to sensitive applications (e.g. authorisation servers) are successful. If the CPS allows the initiation of transactions without secure online *authorisation* (e.g. *card not present*) fraudsters could easily take advantage of such situations when appropriate security measures or limitations are not in place.

- Without having in place appropriate security measures and facilities to monitor activities of cardholders and card acceptors, it is very difficult to limit the impact of fraud. Therefore, measures like card revocation lists, rapid change of secrets, transaction limits and so on could be implemented to mitigate such risk, in overall coherence with the security policy.
- Each CPS component can only process or store a certain amount of data. If this limit is reached, availability and integrity problems may occur at peak times or on peak days.
- Disputes between actors cannot be solved if transparent, easily accessible information and evidence are missing. Confidence in and acceptance of the CPS would be endangered if such situations occurred too often.

- **Secure clearing and settlement**

- Problems within clearing and settlement processes could lead to financial losses, especially for the acquirer and/or card acceptors. These could occur on account of inadequate operational reliability, security and business continuity. An adequate degree of security, operational reliability and availability in line with both the risk level and contractual obligations (e.g. settlement deadlines) is important to ensure integrity of all data exchanged within the clearing and settlement processes.

- **Business continuity**

- Disasters or major events affecting critical business processes could result in prolonged unavailability. If business continuity plans are missing or inadequate, availability, confidentiality and integrity problems could occur and could result in financial losses.

- **Control of outsourcing**

- If some functions of the CPS are outsourced, service level agreements may not be complete or precise enough and/or the inadequate monitoring of the provision of services may cause security breaches. Detailed service level agreements and a penalty system in the event of fraud, processing errors or a loss of availability can, for example, help a proper management of outsourcing.
- The concentration of activities among a reduced number of outsourcers could pose serious problems of availability and dependence.

STANDARD 4: THE CPS SHOULD HAVE EFFECTIVE, ACCOUNTABLE AND TRANSPARENT GOVERNANCE ARRANGEMENTS

KEY ISSUES

4.1 Effective, efficient and transparent processes should be defined and implemented when:

- making decisions about business objectives and policies, including access policies on issuers and acquirers;
- reviewing performance, usability and convenience of the CPS; and
- identifying, mitigating and reporting significant risks to its business.

4.2 There should exist an effective internal control framework, including an adequate and independent audit function.

EXPLANATORY MEMORANDUM

- A CPS has a wide variety of stakeholders, including issuers, acquirers, cardholders and card acceptors.
- Adequate and transparent governance arrangements are vital to ensure that the CPS is able to take decisions appropriately, balancing the needs of all stakeholders. For example, transparent access policies contribute to the awareness of participants and customers regarding the functioning of the CPS and the risks they may face. They also help to ensure that a CPS sustains market dynamics and innovation, manages the conflicts of interest that can arise from the involvement of such a wide variety of stakeholders and reacts promptly and effectively to a crisis situation. Equally important to transparency is the establishment of fair admission/exit criteria. This is especially true in cases where, owing to a market failure, insufficient alternatives are available.
- The availability of the CPS from a customer perspective is vital for the smooth functioning of the CPS. It is important from a governance perspective to evaluate

and anticipate the evolution of transaction flows to ensure availability of the scheme even at peak times and dates. If the CPS governance authority fails to collect and monitor information relating to customer confidence regarding whether or not the CPS is meeting its standards, whether these are explicit or implicit, it might fail to meet customer needs and expectations. This could also lead to disputes among the actors and/or problems arising as a result of poor performance. These aspects – if properly addressed – help to preserve customer confidence in the CPS.

- Effective risk management processes ensure that the CPS is able to prevent, detect and react appropriately to events. Effective risk management should appropriately address the risks in the context of speed of technological change, changing customer expectations, proliferation of threats and vulnerabilities. They also ensure that the most significant risks are identified and regularly reported to the senior management of the CPS.
- Effective internal control processes are essential in order to prevent and promptly highlight any disruptions and instances of fraud resulting in loss of confidence in the CPS. Internal review processes should ensure that the causes of errors, fraud and inconsistencies are swiftly identified and that appropriate remedial action can be taken without delay. A regular independent audit provides additional assurance as to the soundness of the arrangements in place.

STANDARD 5: THE CPS SHOULD MANAGE AND CONTAIN FINANCIAL RISKS IN RELATION TO THE CLEARING AND SETTLEMENT PROCESS

KEY ISSUES

5.1 The CPS should identify the financial risks involved in the clearing and settlement arrangements and define appropriate measures to address these risks.

5.2 The CPS should ensure that all selected clearing and settlement providers are of sufficient creditworthiness, operational reliability and security for their purposes.

5.3 If there are arrangements to complete settlement in the event of an issuer defaulting on its obligations, it must be ensured that any resulting commitment by an actor does not exceed its resources, potentially jeopardising the solvency of that actor. The CPS must also ensure that actors are fully aware of their obligations under any such arrangement, in line with Standard 2.

- Arrangements may exist to complete settlement in the event of an issuer defaulting on its obligations in order to contain credit and liquidity risks. This can be beneficial both in terms of reducing financial risks and improving the clarity and certainty of potential financial risk for all actors, especially in multilateral net systems where settlement could gridlock and/or create an unexpected shortage of liquidity.

EXPLANATORY MEMORANDUM

- The finality of card payment transactions and the financial stability of the CPS itself may be jeopardised if the CPS governance authority does not assess – and mitigate as appropriate – the financial risks involved in the clearing and settlement process. Where the clearing and settlement process uses payment systems within the oversight scope of a central bank, the CPS governance authority can use this fact in its risk assessment.
- A financial default or an operational/security failure by a settlement provider could lead to significant, although not systemic, losses. This is especially important if the CPS governance authority or its actors carry positive balances with the settlement provider during the process. It is therefore important that the CPS governance authority regularly monitors the creditworthiness and operational/security reliability of the clearing and settlement provider and also ensures that contracts with them contain clauses for early termination.

ANNEXES

OVERVIEW OF CARD PAYMENT SCHEMES

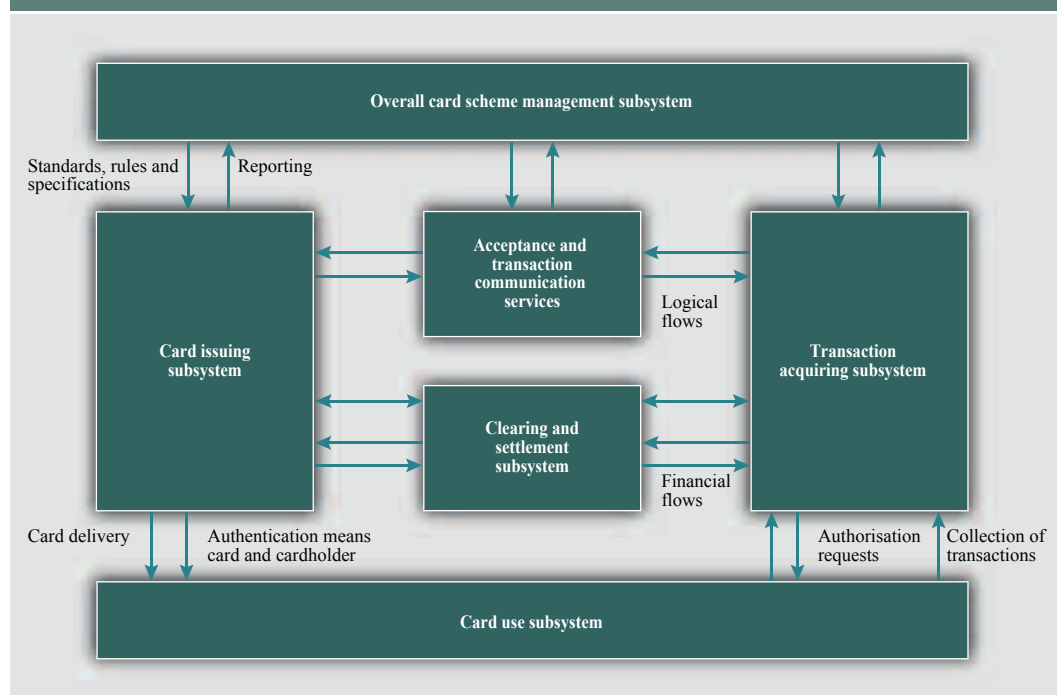
CPS systems can be broken down into six main components:

- overall card scheme management;
- card issuing;
- card usage;
- transaction acquiring;
- *acceptance* and transaction communication services; and
- clearing and settlement.

The different subsystems present in any CPS (see figure) are presented below. The subsystems are explained on the basis of the tasks they carry out and not the physical elements or entities that carry them out. It must be clarified that, within each subsystem, several entities may be involved in performing the related tasks, for example, where entities other than card issuers are involved in the card issuing subsystem.

- The *overall card scheme management subsystem* is dedicated to the governance aspects. Business functions are, for example, definition of standards, rules and specifications or selection and adoption of existing ones, policies concerning access, competition, pricing, fraud prevention and governance, etc.
- The *card issuing subsystem* deals with cardholder and card management, card manufacturing and personalisation, data processing, response to authentication and authorisation requests. Activities related to card issuing are carried out by card issuers and delegated third-party service providers.
- The *card use subsystem* reflects the usage of a card by a cardholder to pay an amount of monetary value to a card acceptor. It includes all the functions necessary to the transaction *acceptance* process (card and/or cardholder authentication, authorisation requests).

Figure Card payment scheme



- The *transaction acquiring subsystem* deals with the management of card acceptors, the forwarding of authentication and authorisation requests and of accepted transaction information, the management of *terminals*, including manufacturing. Activities related to card acquiring are carried out by card acquirers and delegated third-party service providers.
- The *acceptance and transaction communication services subsystem* consists of the technical elements enabling the *acceptance* process and the exchange of card transaction information between the subsystems.
- The *clearing and settlement subsystem* concerns all activities and infrastructure needed for the bilateral or multilateral clearing and settlement of card transactions.

GLOSSARY OF TERMS

Acceptance: the process for checking whether the transaction complies with the CPS Rules (e.g. the card has not expired or been revoked, the identity of the card and its card holder is correct and the financial limits of the cardholder have not been exceeded).

Accepting device: any device that processes payment card transactions where the card and cardholder are present.

Actors of a CPS: governance authority, service providers, vendors and customers (i.e. card acceptor and cardholder).

Authentication: the methods used to verify the origin of a message or to verify the identity of a participant connected to a system.

Authenticity: the property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.

Authorisation: the process initiated by a POS or ATM by which a request for the transfer of funds for the benefit of the card acceptor and ultimately paid for by the cardholder, is approved or declined. In general, the decision to approve or decline a transaction is taken by the issuer, or by a third-party on behalf of the issuer.

Card acceptor: a retailer or any other entity, firm or corporation that enters into an agreement with an acquirer to accept payment cards, when properly presented, as payment for goods and services (including cash withdrawals) and which will result in a transfer of funds in its favour.

Card acquirer: credit institution, payment service provider as defined in the Payment Services Directive or other undertaking and that enters into a contractual relation with a card acceptor and the card issuer via the CPS, for the purpose of accepting and processing card transactions. In some cases, the card acquirer may act as a card acceptor itself.

Cardholder: the person or entity that enters into an agreement with an issuer in order to obtain a payment card. Through this agreement, the card holder is authorised to use the card for its intended purposes (e.g. payment guarantee, cash withdrawal, cheque guarantee, identification, multi-applications etc.).

Card issuer: the credit institution (or more rarely other undertaking) that is a member of a card scheme and that enters into a contractual relation with a cardholder that results in the provision and use of a card of that CPS by that cardholder.

Card-not-present payment: a payment transaction based on card-related information without the card being physically presented to the merchant i.e. mail order, telephone order, Internet.

Card payment scheme: for the purposes of the oversight framework, a card payment scheme is the set of functions, procedures, arrangements, rules and devices that enable a holder of a payment card to effect a payment and/or cash withdrawal transaction with a third party other than the card issuer. The oversight framework covers the entire payment cycle, i.e. the transaction phase (including the manufacture of payment instruments and the processing of data) and the clearing and settlement phase; it accommodates concerns relating to both the retail payment system and the payment instrument used.

Confidentiality: the quality of being protected against unauthorised disclosure.

Cryptographic algorithm: a mathematical function that is applied to data to ensure confidentiality, data integrity and/or authentication. A cryptographic algorithm, using keys, can be symmetric or asymmetric. In a symmetric algorithm, the same key is used for encryption and decryption. In an asymmetric algorithm, different keys are used for encryption and decryption. See also cryptographic key.

Cryptographic key: a mathematical value that is used in an algorithm to generate cipher text from plain text or vice versa. See also *cryptographic algorithm*.

Customers of CPSs: the parties – the cardholder and the card acceptor (vendor) – using the services of a CPS.

Embossed: characters raised in relief from the front surface of a card.

Governance authority: the CPS actor who is accountable for the overall functioning of the CPS and its coherence; it should ensure that all other actors follow the rules and apply relevant measures. The standards allocate responsibility directly to the governance authority. The CPS rules may allow delegation of some of these responsibilities to other actors of the CPS. The governance authority should clearly define such cases and ensure that the choices of the other actors of the CPS are compliant with the overall CPS standards. The governance authority could be a specific organisation or entity or be represented by decision-making bodies of cooperating schemes.

Integrity: the quality of being protected against accidental or fraudulent alteration or the quality of indicating whether or not alteration has occurred.

Off-line transaction: a transaction processed and approved/declined at an *accepting device* on the basis of communication between the card and the accepting device without actually contacting the issuer (or its agent).

On-line transaction: a transaction that is approved or declined at an accepting device following a real-time dialogue between the acquirer and issuer (or its agent). This requires that the accepting device is connected on-line during the transaction phase to the acquirer, to send the request and to receive the response.

Outsourcing: a situation where a service provider contract with a third party in order

to fulfil its own responsibilities defined by the CPS. In general, each service provider is fully responsible for all outsourced activities. Such a service provider must ensure that all outsourced services and activities are provided, controlled and monitored in a way, as if they were operated by the service provider himself.

Payment card: a device that offers the cardholder the ability to make payments for goods and services, either at an accepting device or remotely (via mail order, telephone order, Internet – these are known as “card-not-present” transactions) or to access cash at an ATM.

PIN (personal identification number): a secret code which the cardholder may need to use for verification of identity (CPSs generally use a 4 numerical number).

Personalisation of a card: loading all information necessary for the use of the card for payment, cash.

Secret: information which can only be known to authorised users in order to enforce the security policy.

Service provider: the actors who participate with internal or external resources in services offered to customers of the CPS. Service providers include: issuers; card manufacturers; acquirers; terminal manufacturers; maintenance operators; *switches* (transaction collectors which dispatch further information); communications network service providers; clearing providers (payment system operators); and settlement providers. In some cases, an entity may play different roles: for example, in the case of three-party schemes the issuer and acquirer are the same entity. Given the relevance of issuing and acquiring in CPSs, the document often refers to “issuer” and “acquirer” as “participants”.

Switch: the routing centre that transfers authorisation requests, approvals and transaction information to the appropriate receiver.

Terminal: a type of accepting device.

Transaction phase: this phase encompasses acceptance and authorisation of a card as well as the exchange of the data used as input for the clearing and settlement process.

