Canadian Payments Association

Association canadienne des paiements

1212 - 50 O'Connor
Ottawa, Ontario
K1P 6L2
(613) 238-4173
Fax: (613) 233-3385

PRINCIPLES AND GUIDELINES FOR PAYMENTS OVER OPEN COMMUNICATION NETWORKS

Approved:

October 5, 2000

I. INTRODUCTION

The proliferation of payment technologies is having a tremendous impact on the payments system. To guide the development of such technologies, the Canadian Payments Association (CPA), in collaboration with its members and stakeholders, has developed a set of principles and guidelines for financial institutions as a framework for payment services over open communication networks. In this document, "open communications networks" refers to those forms of communication infrastructure, technology and systems that permit the processing and transmission of electronic messages or data in a manner that can be accessed and used by everybody.[1] These types of communications networks include the Internet, wireless, digital, analog, and fibre optics. "Payments over open communications networks" denotes the transfer of funds initiated through any of the above systems so as to order, instruct or authorize a financial institution (FI) to debit or credit an account held by itself or at another financial institution.

II. THE CPA AND ITS PUBLIC POLICY OBJECTIVES

The CPA was created by an Act of Parliament in 1980 with a statutory mandate to: a) "*establish and operate a national clearings and settlements system";* and b) *"plan the evolution of the national payments system"*.[2] Although some changes in the CPA's mandate are expected in view of proposed legislation, the essence of the existing mandate is not expected to change significantly, and the public policy objectives should, for the most part, remain the same. CPA membership is composed of banks, trust and loan companies, credit union centrals and other deposit-taking financial institutions (FIs).

The CPA currently operates the United States Bulk Exchange (USBE) which may be used for settlement in U.S. funds, the Automated Clearing Settlement System (ACSS), and the Large Value Transfer System (LVTS) which may be used for settlement, in Canadian funds at the Bank of Canada.

The broad forces of change have led to tremendous developments in the form of payments instruments, technologies and systems that have had, and continue to have, a significant impact on the payments communications processes, as well as the payments environment generally. The primary objectives of the CPA in relation to such payments systems and the communications processes they employ, are that they must:

(i) be secure, confidential, efficient, effective, accurate and reliable;

(ii) recognize the interests of all participants and users of the payments system; and

---

[1]Depending on the access authorization, a distinction is made between "open" communications networks (i.e., networks that can be used by everybody), and "closed" communications networks where only certain users/closed user groups are able to access the systems or parts of the information offered on the systems through the use of passwords and encryption. The primary difference between open and closed networks is the authorization of access to such networks, and not transfer technology. See U. Sieber, "Technical Control Possibilities for the Prevention of Criminal Content in Computer Networks" http://www.jura.uni~wuerzburg.de/sieber/control/Control_eng(1).htm

[2]In the recently tabled federal financial institution legislation Bill C-38: *An Act to Establish the Financial Consumer Agency of Canada and to Amend Certain Acts in Relation to Financial Institutions*, the objects of the CPA would now be three-fold, namely: a) establish and operate national systems for the clearing and settlement of payments and other arrangements for the making or exchange of payments; b) facilitate the interaction of its clearing and settlement systems and related arrangements with other systems or arrangements involved in the exchange, clearing or settlement of payments; and c) facilitate the development of new payment methods and technologies (Section 216(1).

(iii) ensure that risks and liabilities are clearly allocated and disclosed to all parties involved.[3]

By establishing a set of principles applicable to payments over open communication networks, the CPA strives not only to achieve these objectives, but also to guide new payment systems in such a manner that would increase efficiency of commerce and payments generally; encourage the shift from paper items to e-commerce payment alternatives; promote confidence and minimize the likelihood of erroneous and illegitimate transactions.

III. PRINCIPLES FOR PAYMENTS OVER OPEN COMMUNICATIONS NETWORKS

A. WHAT ARE PRINCIPLES?

The CPA principles on payments over open communication networks are high-level fundamental doctrines intended to provide a basis for the introduction and implementation of payment schemes that utilize open communication networks, to guide the development of such schemes or technologies, and to facilitate the attainment of the Association's mandate. As such, this document presents a set of principles which state the fundamentals that need be adhered to; and accompanying guidelines for, and attributes of, payment schemes conducted over open communications networks.

B. PRINCIPLES

Any system, technology or device for making or facilitating payments over open communication networks should, as a minimum, meet the following principles:

1. ESTABLISH TRUST AND CONFIDENCE

1.1 Trust management framework

Establishing trust and confidence is the pre-eminent principle. All of the remaining guiding principles identified below support the attainment of this key objective. The utilization of open networks for electronic commerce has shifted the focus for trust from the traditional physical infrastructure to electronic relationships. **Any mechanism intended to facilitate payments over open communication networks must ensure that the traditional trusted relationships provided by financial institutions are extended electronically** (i.e., it must exhibit attributes of authentication, non-repudiation, and integrity of information). It must, therefore, provide the base and define the management framework for electronically extending this trust between organizations and users.

1.2 Security and operational reliability

To ensure the accuracy and integrity of payment transactions, the systems must have rigorous security standards that reflect the transaction values involved. Although the provision of maximum security may translate to high costs, inadequate security standards would result in even higher costs (e.g., cases of security breaches, litigation, etc. and minimal consumer confidence in the system). A prudent and thoughtful balance is needed. **Thus, a high degree of operational resilience and**

[3]The CPA, *Principles Applicable to Shared Electronic Point of Service Environments*, June 15, 1997, p. 2.

security beyond the mere provision of reliable technology and adequate backup of all hardware, software and network facilities must be in place.

1.3 Sound alternative contingency arrangements

Payment transactions over open networks are information-based, intangible and electronically conducted. Computers used for such transactions may experience technical problems. For example, there could be a total system breakdown, or unauthorized entry (hacking) into the system that may result in either business disruption, fraud, or total system or network failure.[4] **Thus, an integral part of the arrangements of such systems should be the provision of alternative mechanisms or strategies sufficient to deal with any or all such disruptions should they occur. Adequate back-up capabilities, responsibilities and liabilities in these situations must be properly addressed.**

1.4 Effective Payment

At the heart of all financial transactions is the consummation of payment - exchange of monetary value for goods purchased or services rendered. **In order to facilitate the non-repudiation of such exchanges, payment systems must be designed to ensure prompt payment for duly authorized transactions.** The design of such payment schemes should be done with due consideration for the needs of all system participants (e.g., buyers and sellers), and promote the efficiency, safety and soundness objectives of the payments system as a whole.

1.5 Effective accountability and transparency in governance arrangements

Governance arrangements provide the structure through which overall objectives are set, how they are attained, and how performance is monitored. **Because payments over open networks have the potential to affect the national payment system, the national economy and the economic community, there is a particular need for effective, accountable and transparent governance**. This would provide proper incentives for the CPA Board of Directors and direct participants to pursue objectives that are in the interests of the payments system, its participants and the public more generally.

1.6 Clear redress and dispute resolution procedures

In any payment arrangement, be it traditional or electronic-based, errors and problems may result from a range of factors. Returns and claims are an important part of purchasing and payment processes, and they impact administrative costs and customer relations. **Thus, payment systems that utilize open communication networks must establish and administer an efficient and cost-effective process for identifying and resolving issues that impact the payment process.** The systems must define and implement the required rules and procedures to ensure that all issues are dealt with in a timely and efficient manner.

---

[4]The examples above are by no means exhaustive.

2. ADAPTABILITY AND INTER-OPERABILITY

2.1 Flexibility, portability, scalability and accessibility

The forces of innovation continue to have a tremendous impact on payments and settlements systems. These driving forces have led to the growth of payment instruments and unleashed an information revolution that is affecting the nature and structure of financial services. **Therefore, the technologies and rules used to support the use of applications over open networks must be flexible to accommodate the potential for growth, and also be designed to ensure that they are portable and can adapt to developments in the payments technology marketplace.**

2.2 Technology neutrality and inter-operability

Industry standards currently in use to support payments systems continue to evolve and mature. The ability to support payment transactions over open networks depends largely on the use of robust technologies and standards by all participants. **Technology neutrality will ensure that the technology selected to operate specific payment systems will match the requirements of such systems, rather than adapt the requirements to conform to available or existing technology. Thus, it will enhance the systems' competitiveness and innovative capabilities, as well as enable them to be fully inter-operable with the widest variety of systems and infrastructures.**

3. EFFICIENT AND RISK-CONTROLLED SYSTEMS

3.1 Cost-effectiveness and efficiency

Participants in payment systems that utilize open communication networks have an interest in the systems' efficiency. Typically, there will be a trade-off between minimizing resource cost and other objectives such as speed to market or maximizing safety. While innovation and system design may reduce costs, they may also increase the incidence of risks (i.e., legal and operational) in the system. Given the security-sensitive nature of these types of payments, there is a need to adhere to a set of robust standards that will mitigate these risks. **Thus, the design of payments systems must balance cost-effectiveness and efficiencies with risk considerations, taking account of the overall objectives of the systems.**

3.2 Articulation and minimization of risks and liabilities

Every financial transaction entails some elements of risk. For payments over open networks, risks may be more difficult to detect due to the intangible and information-based nature of the transactions. It is not uncommon to find spurious and erroneous transactions that result from either honest human error or, in some cases, calculated fraud. So also are there cases of computer glitches, malfunction, or even institution/operator failure. **Therefore, the relative assignment and extent of liability with respect to all participants in and users of the systems, as well as the risk management processes, must be well articulated and disclosed.**

3.3 Settlement arrangements

Participants may face credit and liquidity risks between the time when payments are accepted for settlement and the time when final settlement occurs. These risks are exacerbated if they extend overnight, in part because a likely time for the relevant authorities to close insolvent institutions is between business days. **Prompt final settlement is encouraged in order to reduce these risks.**

4. WELL-FOUNDED PUBLIC POLICY FRAMEWORK

4.1 National legislation and regulations

Payment systems that utilize open communication networks may offer a variety of differing payments applications (e.g., some payment applications may be only national, others may be geographically unrestricted). **The infrastructure and its resulting payment applications must adhere to the legislation and regulations governing payments and payments-related activities**. Furthermore, the national and international standards for the safety, soundness and efficiency of payments systems should be observed.

4.2 Appropriate participation criteria

Appropriate participation criteria (i.e. for suppliers of payments services) to encourage competition and promote efficient payments systems should be defined and disclosed to all participants. The continued security and integrity of the systems depend on the safe operating practices of all participants. Therefore, participation criteria should reflect the need to protect the systems and their participants from excessive legal, financial or operational risks. **Any criteria for access must, however, be objective.** Also, there should be clearly specified procedures for orderly withdrawal from the systems, either at a participant's request, or following a decision by the system's operators that a participant should withdraw.

It is the CPA's view that adherence to this set of principles will promote confidence in, and ensure the integrity of, payments conducted over open communication networks and will minimize the likelihood of erroneous or unauthorized transactions. In order to foster the attainment of these objectives, the CPA has also articulated guidelines for providers of payments applications.

IV. GUIDELINES FOR PAYMENTS OVER OPEN COMMUNICATION NETWORKS

It is desirable that any system, technology or device for making or facilitating payments over open communication networks be guided by the following:

Security

1. **Logical Security** - Payment schemes that utilize open communication networks should provide logical security by ensuring that all information stored or passed through the network uses highly secure techniques, (e.g., end-to-end encryption) in order to ensure the integrity and confidentiality of all the transactions. Also, the schemes should be subject to regular security risk analyses so as to monitor technological advances proactively and to keep the schemes' security risk analysis up-to-date.

2. **Physical Security** - When information confidential to a participant is required to be entered or displayed in a public environment, the physical environment should allow sufficient privacy to enable such information to be entered or displayed with minimal risk of it being revealed to others. This would enhance confidentiality and privacy of such information, which are crucial elements in the successful conduct of these types of payments.

Authentication

3. **Identification/Authentication** - There should be a secure method, established by the deposit-taking financial institutions, for the positive identification and verification of participants or end-users in the system through the use of various cryptographic techniques. For example, this may be achieved through a secure digital signature in the form of a numerical value which is affixed to a data message and which, using a known mathematical procedure associated with the originator's private cryptographic key, makes it possible to determine that this numerical value has been obtained with the originator's private cryptographic key.

4. **Participant Control** - The payment schemes should allow the end-users or participants to approve or cancel a transaction prior to its transmission and execution in order to encourage participants' responsibility, to safeguard credibility in the marketplace, to provide customer convenience, and to enhance the ability to ensure accuracy of the transactions.

5. **Verification of Transaction** - Payment schemes should allow participants to verify the status of financial transactions - whether the transactions have or have not been completed as expected. The processing of transactions in a timely manner in accordance with the rules that define a particular payment system will facilitate this process. Relevant information on the transactions should be readily available, complete and up-to-date. This would ensure proper authentication and auditability of the transactions.

6. **Technique for Authentication** - Security techniques provide assurance that the individual is appropriately identified. They are used to authenticate the identity of the end-user or participant and are considered to be the equivalent of the participant's signature. To achieve and foster privacy, efforts should be made to ensure that the security technique remains confidential to the participant, and is used by the same to approve each transaction.

7. **Accessibility** - The generation and safe-keeping of either digital signatures or other cryptographic modules used to enhance the security of payments over open communication networks are critically sensitive processes. Modules must be adequately protected so as to guard against having them compromised. Therefore, the signatures/modules should be stored in a secure environment where they can be accessed only by the duly authorized persons.

Transactions

8. **Liability/Risk Management** - Payments over open communication networks, being of an information-based and intangible nature, are inherently risky. A comprehensive and effective risk control and management system that delineates the various obligations, rights, responsibilities and duties of all the participants should be developed. The assignment of liability with respect to participants and users should be articulated and disclosed.

9. **Guarantee** - Where possible, end-to-end guarantee of payment should be provided for duly authorized transactions. Such guarantee schemes should be designed with due regard to the efficiency, safety and soundness of the payments system, as well as the protection of participants' interests.

10. **Recourse** - In commercial payments, errors in transactions may occur from time to time. This being the case, appropriate recourse mechanisms that assign liabilities among participants and provide methods and procedures for redress should be in place, and clearly communicated.

11. **Participant Dialogue** - The interactive dialogue a participant encounters when using payment applications over open networks will vary depending on the application and the specific elements of individual implementations. The prompts of any given application should use plain language to ensure clarity and be consistent throughout the system. Dialogue should be standardized to the extent possible so as to facilitate the adoption by participants.

12. **Message Standards** - Any messages transmitted should be reliable, standardized in format, and contain a sufficient set of transaction information necessary to facilitate and complete payment. All parties involved in the passing of messages should adhere to stringent security standards and a uniform message format. In order to foster integrity, measures should be in place to ensure that the important components of a transaction cannot be changed between the source and the destination without detection, or accidentally or intentionally destroyed or disclosed to an unauthorized party.

13. **Control of Messages** - It is important to ensure that all payment instructions received are legitimate and authorized by the appropriate participant. The message environment should be one in which adequate controls are in place to ensure the security and integrity of the data held and processed by that environment.

14. **Privacy and Confidentiality** - Participants in a payments scheme that utilize open communication networks should pass only the financial and other supporting information for completing, tracing, and correcting a financial transaction. All financial information should be held and treated as private and confidential by the scheme participants except where disclosure is required by law, court order, or with the permission of the owner of the information.

15. **Transaction Records** - At the time of a transaction, and if the transaction involves a transfer of funds to or from a participant's account, the participant should be offered a record of the transaction that is reproducible, so as to facilitate the management of finances, and to expedite the process of resolving any disputes or errors.

16. **Inquiry and Complaint Handling** - The responsibility for handling inquiries and complaints arising from payments made over open communication networks should be clearly defined. All parties to a financial/payment transaction should be prepared to assist in the resolution of inquiries or complaints relating to the payment transaction in a timely manner.

17. **Tracing -** When a transaction involves a transfer of funds to or from a participant's account:

a) each participant involved in the transaction should have the right to request tracing information by approaching its own financial institution and the latter should respond in a timely manner;

b) a transaction logging method should be in place to ensure that such transactions can be traced, both forward and backward through the parties to the transaction, including:

i) a method to identify each transaction uniquely;

ii) message logs sufficient to reconstruct the component messages for tracing and audit purposes; and

iii) a facility to permit the identification of each participant through which the message passes; and

c) minimum time requirements for record retention should be established, and should preferably be uniform throughout the network or system.

18. **Contingency Arrangements** - If practical, it is desirable that alternative methods of effecting transactions should be in place in the event of a system failure or unavailability of any component of the payments processes. Although understood to be second best, standardized contingency arrangements or methods of effecting transactions should be available in case of disruptions to the system.

19. **Settlement** - Where settlement agents are required to complete a transaction, settlement arrangements, and their risks, should be well assessed and communicated by networks and their participants, prior to finalizing any such arrangements.

In addition, the Direct Clearer(s) involved should engage in an in-depth assessment of the settlement risks involved. This would ensure the understanding and mitigation of counterparty risks, including the risk that any entity for which a Direct Clearer is settling might fail to meet its payment/reimbursement obligations.