SECURITY OF ELECTRONIC MONEY

Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries

Basle

August 1996

ISBN 92-9131-119-7

FOREWORD

In November 1995, the central bank Governors of the Group of Ten (G-10) countries commissioned a series of studies on specific issues related to electronic money, in view of the potential importance of this new form of money and its implications for monetary policy, consumer protection and payment systems. These studies were carried out by the Committee on Payment and Settlement Systems (CPSS). For the examination of the security aspects of electronic money schemes the CPSS sought the assistance of the Group of Computer Experts, which established for that purpose the Task Force on Security of Electronic Money, chaired by Mr. Israel Sendrovic from the Federal Reserve Bank of New York. At their meeting in July 1996 the G-10 Governors discussed the various reports that had been commissioned and agreed on the publication of the present report on Security of Electronic Money. The report is not necessarily intended to represent the official views of the Governors.

The Task Force on Security of Electronic Money met regularly between January and March 1996 and during that period also organised meetings with potential suppliers of various types of electronic money products. The intention was neither to cover the entire spectrum of products nor to assess individual systems, but to understand and evaluate the relevant security aspects relating to electronic money.

This report highlights the main design features and functional aspects of electronic money products and analyses the technical risks specific to these products. It also describes the possible security measures that can be relied upon to prevent, detect and contain fraud.

One conclusion of the report is that a range of measures exist which would enable the risks inherent in using these products to be controlled. However, there is no single security measure or set of measures that can be said to provide a guarantee of complete protection. It is the combination of measures together with the rigour with which they are implemented and administered that will serve to reduce risks most effectively. The report also underlines the importance of an overall approach to risk management, which might involve assessments by independent bodies.

It should be stressed that the report is based on knowledge of schemes that are currently under development or at a pilot stage. The analysis contained in the report as well as its conclusions might therefore need to be reviewed in the future in the light of expected technical and operational innovations and adaptations. Nevertheless, it is felt that the report can contribute to improving the general understanding of the technical aspects of electronic money products and to raise the awareness of the specific risks that might be involved and of the security measures available to counter those risks. The report does not evaluate any specific product.

Mr. Sendrovic and his colleagues are to be congratulated on having completed this important undertaking within tight time constraints. Able assistance in editing and publishing the report was provided by the BIS.

William J. McDonough, Chairman
Committee on Payment and Settlement Systems

Henri J. Barbé, Chairman
Group of Computer Experts

Table of contents

Members of the Task Force on Security of Electronic Money established by the Group of Computer Experts

Chairman
Mr. Israel Sendrovic
Federal Reserve Bank of New York

Bank of England	Mr. Geoffrey Prior
Deutsche Bundesbank	Mr. Georg Heine
Bank of Italy	Mr. Fabio Cecchi
Bank of Japan	Mr. Toru Asada
Netherlands Bank	Mr. Simon Lelieveldt
Board of Governors of the Federal Reserve System	Ms. Heidi Richards
Bank for International Settlements	Mr. Yves Carlier

Mr. Paul Van den Bergh of the Bank for International Settlements also took part in some of the meetings of the Task Force and contributed to the preparation of the final report.

EXECUTIVE SUMMARY

The Task Force on Security of Electronic Money was established following a workshop on retail payment systems developments held in October 1995 by the Committee on Payment and Settlement Systems of the G-10 central banks. The Task Force's objectives were to analyse the technical risks and security features of electronic money products and provide a preliminary assessment of the security measures.

The Task Force primarily examined consumer-oriented stored-value payment products, a few of which have already been launched in large-scale pilot programmes in various countries; others are expected to be widely introduced in 1996 or 1997. Through interviews with suppliers, the Task Force identified general models of electronic money products and specific characteristics that are relevant to security. The Task Force found that the logical design chosen for the stored electronic "value", as well as the conditions under which such money balances can be transferred to other users, provide the basic framework for examining security measures in the various stored-value products. In addition, the Task Force distinguished between card-based systems, which are implemented through a specialised computer hardware device, typically a "smart card" (a plastic card containing a microprocessor chip), and software-based systems, which employ specialised software installed on standard computer hardware using standard operating systems.

Security risks to electronic money systems could arise in the consumer or merchant domains and in the financial institution domain, as well as in network communications. Attacks on the security of electronic money systems would most probably be attempted for financial gain, but could also be aimed at malicious disruption of the system. Specific attacks could be instigated through attempts to duplicate or steal genuine consumer or merchant devices, to create fraudulent devices or messages that are accepted as genuine, to alter data stored on devices or in messages transmitted between devices, or to alter software functions on a device from their intended purpose. Malfunctions of devices or communications systems could also lead to accidental losses.

The Task Force found that various security measures have been developed to protect the integrity, authenticity and confidentiality of critical data and processes of electronic money products. One critical safeguard for card-based systems is the degree of tamper-resistance of the microchip embedded in the card or other device. Tamper-resistant features of these devices provide a significant advantage for card-based systems over software-based systems in terms of technical security, but also add significantly to their production costs. Such features make it extremely difficult and costly to observe or change critical data stored on a chip without proper authorisation, or to alter the operating system or software application functions.

Cryptography is the other critical safeguard for card-based systems and, indeed, the primary safeguard for software-based systems. Cryptography is commonly used in electronic money systems to authenticate devices and messages and to protect data from unauthorised observation or alteration. The security of the cryptography used depends on the strength of the algorithms, the length of the cryptographic keys and a sound key-management structure, which governs the life cycle of keys and the relationship between them. In the future, electronic money systems may migrate towards use of asymmetric cryptographic functions, which currently require more costly crypto-processor chips that may reduce the speed and reliability of transactions. Cryptographic key lengths used in electronic money products are also expected to increase as processing speeds rise.

All the electronic money products examined by the Task Force would establish central system operators (in some cases, the issuer or issuers) to monitor the system on an ongoing basis for attempted security breaches. Monitoring and traceability of individual transactions and the maintenance of cumulative records on individual devices or in a central database serve to enhance the security of the products. Other mechanisms to help detect and contain instances of fraud are also envisioned through the use of statistical analysis of transaction patterns, periodic interaction by devices with the central system and the hot-listing of suspect devices. Limits placed on the maximum

balances of electronic money devices and the duration of validity of balances or devices also serve to deter fraud as well as to contain any resulting losses.

Transferability of electronic "value" directly between users' devices has implications for security. In general, the fewer consecutive transfers allowed without interaction with a central system operator, the greater the ease of detecting fraudulent activity. However, it is the potential unavailability of transaction information for security monitoring purposes, rather than the transferability feature itself, which may pose greater challenges to security. A range of additional security measures may also be implemented to help compensate for any loss of information that results from transferability.

The Task Force found that the technical security measures designed to protect issuers and other participants in electronic money systems from fraud may also serve to limit the usefulness of these products for criminal activities such as money laundering, particularly when compared with existing payment instruments. In terms of the privacy of consumer payment transaction information, electronic money products could have differing impacts, depending on how the products are actually implemented and used.

Overall, the Task Force's impression was that electronic money systems, particularly those implemented with hardware-based security, can be designed with an adequate level of security relative to other common forms of retail payment. However, there is no single security measure or set of measures that can be said to be sufficient for a particular product. It is the combination of measures, together with the rigour with which they are implemented, that will serve to reduce risk most effectively.

Moreover, while the security designs of most electronic money systems share many common features and international technical standards have been established for certain of these features, a wide range of options is available in terms of the specific implementation of products. These options present trade-offs for product developers in the areas of cost, functionality, speed and reliability. The degree of emphasis on these other considerations will have important implications for the level of security ultimately chosen. As a result, the security features of electronic money systems can be expected to undergo fairly rapid evolution as products are introduced and tested in the market.

While the electronic money suppliers interviewed by the Task Force have focused considerable attention and resources on the technical security of their products, security assessments conducted thus far have been partial evaluations of specific aspects of a product, rather than comprehensive security risk assessments of the entire system. The Task Force concluded that an integrated, overall risk-management approach to security, including independent security assessments, is an important component of the security of these new products.

1. INTRODUCTION

1.1 Background

The Task Force on Security of Electronic Money was established following a workshop on retail payment systems developments held in October 1995 by the Committee on Payment and Settlement Systems (CPSS) of the G-10 central banks. Participants at the Frankfurt workshop agreed that the security of electronic money products could raise a number of issues of significant concern to central banks, particularly if such products become widely used. The potential for counterfeiting and fraud could pose significant financial risks to institutions issuing payment obligations in these systems as well as to other participants. As a result, the Chairman of the CPSS recommended further investigation and analysis of the technical security aspects of electronic money, under the auspices of the Group of Computer Experts (GCE), as well as further research work on several other topics. The report prepared by the Task Force on the Security of Electronic Money thus complements other

studies commissioned by the CPSS and the G-10 Governors on the implications of electronic money. This report was reviewed at the July meeting of the G-10 Governors who agreed to its publication in the hope that the report would contribute to the general understanding of technical and security issues relating to electronic money.

1.2 Objectives and limitations

The Task Force's objectives were to analyse the technical risks and security features of electronic money products and, to the extent possible, provide a preliminary assessment of the security measures. The Task Force also considered technical aspects of electronic money products that may affect their potential for use in money laundering or other criminal activity. In both of these areas, the Task Force considered the likely risks and security measures relative to existing methods of payment, although such comparisons are difficult given the current early stage of development and implementation of electronic money products.

The Task Force limited its inquiry to technical matters and did not examine financial, legal or regulatory issues related to the security of electronic money products. Similarly, questions of liability for fraud or counterfeiting, that is, whether merchants or consumers would bear losses for counterfeit electronic money in addition to the issuers or other sponsors of the product, were not addressed. The assignment of such liability could create important economic incentives for security and thus could raise policy issues, but these issues are well beyond the scope of this report.

Importantly, the Task Force did not attempt to judge the adequacy of the security of particular products or to recommend particular security measures or design features as being necessary or sufficient. A process of rapid development and evolution is currently under way for all products analysed by the Task Force, and many aspects of the technology require highly specialised expertise and equipment to make a complete assessment of their security features. The Task Force's report is instead intended to describe the spectrum of security measures that have been developed to address security risks and analyse relevant considerations in their implementation. In addition, the report may help to develop a preliminary framework for central banks and potentially others to use in evaluating security measures as well as the policies and procedures adopted by institutions in this area.

The Task Force examined the issue of privacy of consumer information primarily as it relates to the use of confidential information for fraudulent purposes. The Task Force also investigated the reliability of products against accidental breakage or other system failures to the extent that this was possible given that most products have only advanced as far as the test or limited pilot phase.

1.3 Scope

The term "electronic money" has been used in different settings to describe a wide variety of payment systems and technologies. "Stored-value" products are generally prepaid payment instruments in which a record of funds owned by or available to the consumer is stored on an electronic device in the consumer's possession, and the amount of stored "value" is increased or decreased, as appropriate, whenever the consumer uses the device to make a purchase or other transaction. By contrast, "access" products are those typically involving a standard personal computer, together with appropriate software, that allow a consumer to access conventional payment and banking products and services, such as credit cards or electronic funds transfers, through computer networks such as the Internet or through other telecommunications links.

The Task Force focused its efforts on stored-value products, which comprise stored-value cards, or "electronic purses", and similar products that utilise computer networks, sometimes referred to as "digital cash" or by any number of product names. The Task Force found that many proposed

products have attributes of both stored-value products and access products. Thus, much of the analysis of security aspects is applicable to certain types of access products as well as to stored-value products.

The Task Force determined that a relevant distinction for purposes of assessing security features is not whether or not a particular product can be used over a computer network, but rather whether the product's security is based on specialised tamper-resistant hardware (together with self-contained software) or, alternatively, on software installed on standard personal computer equipment. These two categories are termed "card-based" and "software-based" products in this report.

The scope of the study was limited to the analysis of products that are currently approaching their commercial launch date. While an array of potential products has been proposed and publicised, in many cases these products are still in the early design or pilot phases; as a result, insufficient information is available to assess their security features. In the area of software-based stored-value systems, in particular, fewer proposed products are nearing commercial introduction than in the case of stored-value cards; thus the Task Force was unable to examine in any detail the specific security features and likely implementation aspects of such products. It should be noted that software-based products that are most likely to become commercially available in the near future for use over open computer networks would function as access products to credit card accounts or bank deposit accounts; suppliers of these products were not interviewed by the Task Force.

1.4 Methodology and report structure

The Task Force identified the major suppliers or developers of electronic money products in the G-10 countries and invited them to make presentations to the Task Force on the security features of their products. While not constituting an exhaustive list of products under development, the products of these suppliers were considered to be representative of those most likely to achieve commercial implementation in the next one or two years. Electronic money suppliers were asked to complete a questionnaire on their product's security architecture and procedures. For reasons of confidentiality, this report deliberately avoids identifying specific products or their specific features.

The general information provided through these interviews permitted the Task Force to identify the major structural design features, components and processes of electronic money products, which are presented in Section 2 of this report (and summarised in Annex 2). From the basic structural and functional framework, a set of general risk categories and specific threats were identified, which are described in Section 3. Using the information on the different security measures currently implemented or planned in the electronic money products analysed, the Task Force enumerated the security measures utilised or envisaged in the different products to address the risks and vulnerabilities identified. Section 4 summarises the range of security measures that the Task Force observed in the products analysed. The Task Force identified measures that could prevent the risks perceived, permit participants to detect activity in the event that prevention is unsuccessful, and then contain the resulting losses. These measures are also summarised in a matrix in Annex 3. The Task Force's observations and conclusions regarding the security measures are presented in Section 5. In Section 6, general conclusions regarding the implications of electronic money systems for criminal activities, reliability and privacy are summarised.

The most important technical background information is provided for reference purposes in the annexes. A glossary of terminology used in the report is provided in Annex 1. In addition to the other annexes mentioned above, Annexes 4-7 provide summaries of issues relating to the Internet and its relevance to payment systems, techniques to provide physical security for smart cards, international technical standards regarding the security of electronic money systems, and relevant aspects of cryptographic techniques.

2. PRODUCT STRUCTURE AND FUNCTIONS

2.1 Design features

An understanding of the components and processes of the product under study is vital to any security risk analysis. This section provides a general overview of the electronic money products which the Task Force studied, although many details are necessarily omitted. In general, the Task Force did not encounter any products that could be viewed as true "electronic currency", in the sense of replicating many of the key characteristics of physical currency, which is generally an untraceable, anonymous bearer instrument, readily transferable to any other person in any circumstance without intervention by a third party, although in theory the technology would permit development of such products.

Annex 2 illustrates the general structural model common to most electronic money systems, including participants and their interactions, and certain key structural variations on this model. Physical devices, such as smart cards or personal computers, are held by consumers and by merchants. Merchants interact with consumers and with their acquiring bank or other collection point, such as a third-party payment processor. Issuers receive funds in exchange for prepaid balances distributed to consumers and manage the "float" in the system that provides financial backing for the "value" issued to consumers. In some cases, other intermediaries, such as banks, retailers or service providers, distribute stored-value devices and balances directly to consumers. The system may include a central clearing house or system operator.

Although electronic money products share certain general features, the Task Force also found many major differences as regards design and implementation, as described below.

2.1.1 Basic framework for money storage and transfer

The following characteristics define the fundamental structure of electronic money products and influence the security design of the entire product.

Technical representation of money. The electronic record of "value" stored on a device can be designed in one of several basic ways. Devices can store and manipulate a numeric ledger, with transactions performed as debits or credits to a balance (hereafter referred to as "balance-based" products). Alternatively, devices can store electronic "notes" (sometimes called coins or tokens) that are uniquely identified by a serial number and are associated with a fixed, unchangeable denomination. In the latter "note-based" model, transactions are performed by transferring notes from one device to another, and the balance of funds stored on a device is thus the sum of the denominations of all notes on the device.[1] A third possible approach, which can be thought of as a hybrid of the previous two, is also possible by using what can be thought of as electronic "cheques" that are uniquely identified electronic certificates in combination with a balance. Most of the products examined by the Task Force use a balance-based design.

Transferability. Stored-value products differ in the degree to which participants can undertake transactions with one another without participation by the issuer or another central authority. The Task Force found that free transferability, in which consumers, merchants or banks may make unlimited direct transfers between one another, is a theoretical concept only. In all systems analysed, transferability is restricted, although the degree and types of restriction differ across systems. In the majority of systems analysed, consumers may only make payments to merchants and merchants may only clear these payments or deposit the accumulated balances through their acquiring banks.

---

[1] Note-based systems require a solution to the problem of "making change" or splitting notes if the consumer does not hold the necessary denominations for a particular transaction.

In some systems, consumers may make payments directly to other consumers, but the technological capability exists to restrict these payments through various limits, including the number of such direct transfers or the period of time within which such transfers can occur before communication with the issuer or central operator is required. Greater transferability is not necessarily associated with truncation of transaction information, as discussed later in the report.

2.1.2 Implementation features

Based on the framework given above, the following characteristics define one or more of the major features of the product.

Card-based and software-based products. Most product designs analysed by the Task Force could, in theory, be implemented as either card-based or software-based products. For the purposes of this study, card-based products are defined as those that provide the consumer with a portable, specialised computer device, typically an integrated circuit (IC) card containing a microprocessor chip ("smart card"). The smart card's self-contained operating system and application software are inserted into the chip during manufacturing. In addition to those involving smart cards, card-based products are defined to include those utilising more sophisticated electronic computing devices, such as "electronic wallets", that provide special functions or are capable of greater data-processing capabilities. Owing to their more advanced stage of development, the majority of products analysed in this study were card-based systems.[2]

Software-based systems, in contrast, include those stored-value products that operate via software installed on an industry-standard personal computer, such as a desktop computer or even a smaller portable computer device, supplied by the user and running a standard operating system. Such products are typically designed to be utilised to make payments over computer networks, primarily the Internet. However, many card-based systems have the potential to be used over telephone connections or proprietary or open computer networks, including the Internet. Thus, the relevant distinction between card-based and software-based systems is the implementation of specialised hardware in card-based systems.

Issuer structure. The number and type of issuers - institutions whose obligations are electronically transferred in an electronic money system - is critical from a financial perspective and also affects the technical implementation of an electronic money system. Systems with only one issuer may not need to clear transactions for purposes of interbank settlement, although clearing and settlement would be necessary if other intermediary institutions (distributors and acquirers) were used to distribute and collect funds in the system. In systems with multiple issuers, the card number or a cryptographic "certificate" identifies the issuer, and purchases or loading transactions are typically transmitted to that institution for settlement. Such systems may routinely collect transaction information for financial clearing purposes that may also be useful for security monitoring purposes.

Online authorisation. For some electronic money transactions, online authorisation by a third party is performed before the transaction can be executed, or before the merchant provides its goods or services to a consumer. In general, online transactions require that information on the device or supplied by the user be validated against data held by a central system operator or issuer in secured central databases. For a given product, online authorisation may be used for all transactions or only for certain types of transaction, such as those that debit a bank account. Online authorisation requires an additional communication that can add greatly to the cost and time required for transactions.

---

[2] A variety of other specialised hardware devices have also been proposed, including security calculators, PCMCIA cards, personal digital assistants or specially equipped telephones or screen-phones.

2.1.3 Additional functions

The following features may be optional in their implementation but are also relevant to the security design of an electronic money product.

Information collection. Electronic money transactions generate financial information and security-related information. This information can be stored, temporarily or permanently, by different devices, including consumer devices, merchant terminals, issuers and central system operators. The amount, location and time of information collection depend on the financial structure of the system, the cost of collecting the information and security and privacy considerations. Some systems perform full transaction clearing, in which all transaction details, including the identifying number of each device, are collected as soon as possible after the transaction and transmitted to the issuer. Other systems "truncate" the information provided at the point of sale but store some transaction details in the merchant terminal as well as in the consumer's card or other device involved in each transaction.

Ability to reload devices. Particularly in the pilot or test phases, some stored-value cards are not usable once the initial balance purchased on the card has been expended. Other electronic purse products, as well as products designed for computer networks, are reloadable; that is, the balance on the device can be increased at the consumer's convenience using a variety of payment methods, including direct withdrawal from a bank account, or a cash or credit card payment. Direct withdrawals from a bank account function in a similar manner to cash withdrawals at an automated teller machine (ATM).

Single or multiple currencies. In all the products analysed by the Task Force, electronic "value" stored on devices is denominated in a national currency. In many cases, balances can be held and payments made in several different national currencies. None of the products analysed permits exchange of currencies to take place on the consumer's device without interaction with an external source to provide current exchange rate information; for example, currency exchange could take place at an ATM or, in some cases, at a merchant's terminal.

Single or multiple applications. While some card-based stored-value products are intended to be the only application resident on a consumer's card, in other cases suppliers propose including other payment products, such as debit or credit card functions, on the card. Some projects also involve non-payment applications, such as retail incentive programmes or transport system tokens that would be co-resident on the device. The non-payment applications may be supplied and operated by third parties. Software-based products would, of course, have any number of other applications in addition to the electronic money software residing on the same device.

2.2 Product infrastructure

The processes through which the infrastructure for an electronic money system is implemented can create security vulnerabilities. These processes include the development and production of devices and software, their distribution to consumers and other users and the operation of the central system and network.

2.2.1 Development and production

For card-based products, devices must be designed and tested, manufactured and prepared for use. These processes are described in Annex 5, which also provides an overview of chip card technology. Chip cards are generally manufactured according to a number of international technical standards, as discussed in Annex 6. The operating system for the chip card is generally developed by the manufacturer. The electronic money application may be designed by a separate developer.

During the chip card manufacturing process, the application and operating system coding are physically set into the wiring in the chip module. After testing of the chip modules, a further initialisation ensures that the chip is uniquely identified with a serial number and contains the correct file and directory structures and cryptographic keys. The chip is then embedded in a plastic card. Card personalisation, which may occur at the card manufacturer, at the issuer or at a central system operator, is the process by which individual card and customer data are created and loaded onto the chip.

For software-based products, software must be designed, coded and tested. Design features may be changed or security features upgraded in subsequent generations of the products or releases of the software.

2.2.2 Distribution

In stored-value card systems, issuance of cards to consumers may be accomplished in a number of ways. In some cases, cards are linked to a bank account of the consumer; alternatively, cards may be purchased anonymously at vending machines or using credit or debit cards. Merchant terminals or other devices are typically distributed through acquiring institutions or by a central system operator.

In the case of software-based products, software must be distributed to consumers, merchants and participating financial institutions. Distribution of software may be accomplished through physical transport of diskettes or by transmission between a central system operator and the consumer's device over a telephone connection or computer network; consumers must then install the software on their personal computers.

2.2.3 System and network operation

The electronic money systems analysed by the Task Force establish one or more central computer systems and databases for functions such as control of cryptographic keys, clearing and settlement and monitoring of data for potential fraud. In some systems, many of these functions are decentralised in issuing and acquiring institutions or can be provided by a third-party processor.

For communication purposes, such as for online transactions or collection of transactions from merchants, a variety of methods are possible. Some products use existing credit or debit card clearing networks. Others make use of standard telephone connections or open computer networks such as the Internet for communication between consumers, merchants, issuers and acquirers.[3]

2.3 Transaction processing

Transactions in electronic money systems, whether card-based or software-based, are accomplished through exchanges of electronic messages between computer devices according to predefined protocols which cause the devices to perform certain internal functions. The messages may be transmitted through direct electrical contact, for example between a smart card and a smart-card reader device, through wireless transmission methods or across telecommunications lines, such as those connecting computers in the Internet.

2.3.1 Issuance and loading

Issuance of stored "value" in an electronic money system can occur either prior to or at the time of the "loading" or distribution to consumers. In some electronic money systems, stored-

---

[3] Annex 4 provides background information on the Internet and related security issues.

value balances, "notes" or "cheques" are created by the issuer and distributed to intermediary institutions prior to being distributed to consumers. In other cases, issuance may occur at the time that a consumer initiates a load transaction. Issuance transactions ultimately generate accounting entries in the records of the issuer and may flow through a clearing and settlement process.

Loading of a stored-value card is typically accomplished at an ATM or through the use of a specially equipped telephone; suppliers expect that personal computer-based smart-card readers will also be available in the future for this purpose. If not paid for by cash, credit card or other means, load transactions are generally designed to result in a debit to the consumer's pre-existing bank account that is linked to the card. Most products establish a direct connection to the issuer in the loading process, although offline loading methods, in which completion of processing by the issuer occurs after the balances are loaded, have also been developed. Reloadable products, in some cases, could be designed to permit a small overdraft (negative balance) on the device, which would be covered by a debit to a bank account once the transactions were collected and cleared.

For software-based products, loading is accomplished in a similar manner using messages between the consumer's and the issuer's devices, often transmitted over computer networks. In practice, software-based products for security reasons tend to involve issuance of digitally signed electronic "notes" or "cheques", as described later. Payment to the issuer for such electronic notes is made via direct debit, credit card or other common remote payment methods.

2.3.2 Purchases and other payments

To make a purchase using a card-based product, a consumer inserts a card in a merchant terminal; the merchant (or possibly the consumer) then enters the payment amount.[4] The merchant terminal checks that the card balance is sufficient to complete the transaction, and then instructs the card to debit its stored balance by the payment amount. The consumer's card then instructs the merchant terminal to increase its balance.

A similar process would occur for remote payments via a computer network or telephone, but additional card-reading equipment would be required on the consumer's side. In systems permitting transfers to other consumers, an additional device (such as a "wallet" or telephone) could be used to perform the same function between two cards, whether face-to-face or remotely.

For software-based products, the payment process may depend on the design of the electronic money system as well as the context in which the payment is being made. To purchase an item advertised on the Internet, for example, certain electronic money systems provide for menu-driven software on the consumer's personal computer which automatically prompts the consumer to accept or reject a particular payment based on an electronic invoice sent via electronic mail by the merchant. Alternatively, the consumer may be required to enter the amount and destination of a particular payment. Where a note-based model is used, the serial number of the appropriate number and denomination of notes is transferred from the consumer's device to the merchant’s device using appropriate security protocols, as discussed later.

2.3.3 Deposit, collection and clearing

With some electronic money products, a consumer would have the option of receiving a refund for an unused electronic money balance (or electronic note) and having the proceeds deposited in a traditional bank account, typically one already linked to the device by the issuer. If the bank account were not located at the issuing institution, a clearing and settlement process would be required to redeem the issuer's stored-value obligation.

---

[4] In many card-based systems, suppliers intend to incorporate devices similar to merchant terminals in unattended vending machines.

As in other retail payment systems, electronic money products typically involve a collection process whereby a merchant's account at an acquiring institution is credited with funds received for payments from consumers. In some systems, in which most or all transaction information is truncated at the point of sale, merchants may simply deposit a single accumulated balance (or one balance per issuer) on their terminal through a connection between the terminal and the acquiring institution. For other systems, transaction details are transmitted from the merchant terminal to the acquiring bank, where they are routed to a clearing centre.[5]

In many proposed card-based systems, existing interbank clearing and settlement arrangements such as ATM, debit or credit card networks and systems would be employed. In software-based systems, clearing and settlement mechanisms tend not to be well defined at this stage of their implementation.

3. SECURITY RISKS

3.1 Scope of risks examined

In analysing security risks, the Task Force focused its attention primarily on those aspects of electronic money products that are different from conventional payment instruments such as credit and debit cards and electronic funds transfers. These include, in particular, the use of smart cards and advanced cryptographic techniques. The basic elements of security for electronic payment systems are well established. Thus, the Task Force did not examine in detail issues such as audits and internal controls, separation of employee duties and information, development and testing of hardware and software, and risks in physical production and transportation of devices. However, these aspects of security are the first line of defence against many conceivable security attacks and their importance cannot be overstated.

The Task Force focused on risks and security measures at the level of the consumer or merchant devices. Risks that are internal to an issuer, acquirer, clearing mechanism or central operator could also arise and may create significant vulnerabilities for electronic money systems. For example, an issuer could operate in a fraudulent manner in such a way as to threaten the security of the entire system. Institutions that participate as intermediaries in distributing devices or electronic "value" to consumers could also be a source of risks. In most areas, these security risks have been examined in the context of other payment systems, and administrative controls can be put in place to address them.

The Task Force did not assess security measures aimed at protecting the internal computer systems of issuers or central system operators from outside attacks; Annex 4 describes some of the common security measures that are used to protect computers from attack via network connections, in particular Internet connection. Such risks should not be underestimated; however, they are not unique to electronic money products and thus were considered to be outside the scope of this report. The Task Force did find that electronic money suppliers view transmission of messages between consumers, merchants and central system devices in electronic money system as inherently insecure and open to observation, modification or transmission failure, whether or not the transmission is effected over an open network such as the Internet or by some other method; thus all systems include measures to protect the integrity of messages during transmission.

---

[5] For vending machines, the transaction information can be downloaded periodically onto a portable device, which is subsequently connected to the acquiring bank.

3.2 Fraud risks

The most likely motive for any fraudulent attack would be financial gain. This could be accomplished by creating fraudulent electronic representations of electronic money that are accepted as genuine by the issuer or by other participants, or by stealing devices or data from another participant. If such fraudulent balances could be successfully exchanged for currency or other readily transferable forms of money or physical assets, this would cause financial loss to the issuer or other participants. Alternatively, an attack on an electronic money system might be motivated not by financial gain but by a desire to disrupt a particular system.

The primary areas of vulnerability in an electronic money system were outlined in Sections 2.2 and 2.3. These comprise the devices used in the system, including those held by consumers and merchants, and the messages transmitted between such devices. As with other payment systems, significant areas of risk are to be found in the manufacturing and distribution processes, issuer and acquirer systems and central system operation; however, these categories are not examined in detail in this report.

There are a number of possible methods of attack; general categories of threats are outlined in this section. An important aspect of the security vulnerability of electronic money products is that they are designed for widespread retail usage. Thus, it must be assumed that it would not be difficult for an attacker to obtain large numbers of legitimate software, devices or communications between devices, which would facilitate analysis and reverse engineering of the product. Repeated attempts to compromise a device can be expected even if such attempts result in the destruction of a number of devices.

3.2.1 Duplication of devices

In card-based systems, the method of attack could be the creation of a new device that is accepted by other devices as genuine. The objective would be to duplicate a genuine card, including its existing cryptographic keys, card balances and other data. Alternatively, an attacker could attempt to create a card that would function as a genuine card but would fraudulently contain balances without a corresponding load transaction and payment to the issuer.

Duplicating a smart card or a merchant terminal would involve a number of complicated steps requiring a high level of expertise and resources, as described further in Annex 5. An attacker would need to procure the same type of chip card and load the appropriate operating system, application software and data. An attacker could attempt to reconstruct the operating system and application software by examining genuine cards that might be available through legitimate channels.

3.2.2 Alteration or duplication of data or software

The objective of fraud could be to modify data stored on a genuine electronic money device in an unauthorised manner. For example, if the balance recorded on a device were fraudulently increased without other evidence of tampering or damage to the card, the holder could perform transactions with the device that would appear genuine to the merchant terminal. Another method of attack would be to modify the internal functions of a chip card, such as its accounting procedures, so that calculations would not be executed as intended.

Alteration of data or functions on a device could be attempted through exploiting security weaknesses in the operating system or by physical attacks on the chip itself. In software-based systems, data stored on a consumer's device could be altered directly if not protected by software functions, or software could be modified to allow unauthorised alteration of data by the user. In a note-based system, a user could duplicate data representing electronic notes and attempt to use the notes to purchase goods and services.

3.2.3 Alteration of messages

Attackers could attempt to change the data or processes of a device by deleting messages, replaying messages, substituting an altered message for a valid one or observing messages for the purpose of attempting a cryptographic attack. Communications between devices could be intercepted by outside attackers when sent across telecommunications lines, through computer networks or through direct contact between devices. Interception and retransmission of messages in a software based system that utilised the Internet for transmission would be relatively straightforward, given that standard devices and electronic mail capabilities would probably be used.

An attacker could change the destination device of messages during a transaction by diverting a message sent over a computer network via electronic mail or by removing a smart card from a reader and inserting another with a lower balance. A smart-card reader device could be simulated and used to send false messages to the smart card; alternatively, a fraudulent smart card could be used in a valid card reader, with the intention of causing the card reader device to perform unauthorised functions. Critical data in a message, such as the transaction amount, could be changed and the message then retransmitted to its intended recipient device. Messages authorising the loading of funds from a valid ATM or other terminal could be copied and replayed to a card from a fraudulent terminal. Transaction data transmitted from a merchant terminal to the acquirer could be duplicated in an attempt to receive double credit for the transactions.[6]

3.2.4 Theft

An unsophisticated method of attack would be to steal consumer or merchant devices and fraudulently utilise the balances recorded on them. Data stored on devices could also be stolen via unauthorised copying. For example, in a note-based system, an attacker could intercept messages between a genuine user and an issuer, or insert an unauthorised software program into a user's personal computer that enabled the attacker to copy electronic notes stored or in transmission, and then use the notes to perform transactions. Such a theft would only be detected after the issuer received the fraudulent as well as the genuine copy of the same note for payment, by which time the attacker would probably already have obtained a financial benefit.

As with traditional payment instruments, internal theft within an electronic money supplier could also be an avenue for attack. For example, an employee of an issuing institution could attempt to load balances onto a genuine device while circumventing the normal loading process controls. Employees of manufacturers or issuers could steal devices prior to their being sold or issued to consumers, or could distribute cryptographic keys without authorisation. Product development staff could be bribed to provide confidential product design documentation to outside attackers that might lead to devices being compromised. One of the most significant threats to an electronic money system would be the theft or compromising of the issuer's cryptographic keys by either an inside or an outside attacker.

3.2.5 Repudiation of transactions

Fraud could also be attempted through repudiation of transactions made with an electronic money payment. For example, in remote transactions, such as those conducted over the telephone or via computer networks, a user could fraudulently claim that he or she had not, in fact,

---

6 The security of a system against the risk of duplication or "replay" of messages is sometimes known as "idempotency".

authorised a particular transaction. This could cause losses to the merchant as well as to the institution issuing the particular electronic money product.[7]

3.3 Malfunctions

Electronic money products could suffer from instances of accidental corruption or loss of data stored on a device, the malfunction of an application, such as accounting or security functions, or failures in the transmission of messages. Malfunctions could result from physical or electrical disturbances to a device, or from the interruption or corruption of message transmissions between devices. Such malfunctions could cause losses to a party involved in a transaction if, for example, a malfunction caused changes to stored-value balance data on a device. If exploited by unscrupulous holders before being detected, certain types of malfunction could cause losses to the issuer.

4. SECURITY MEASURES

Security features in electronic money systems, as well as in other payment systems, are designed to safeguard the integrity, authenticity and confidentiality of critical data and processes, as well as to protect against losses due to fraudulent duplication or repudiation of transactions. This section describes the different types of security measures that have been planned or implemented by electronic money product developers to address the risks summarised in the previous section.[8] Annex 3 provides a table summarising these measures and the threats and vulnerabilities they are designed to address.

Security measures can be grouped into several categories based on whether the measure is designed primarily to prevent, detect or contain threats. The primary objective of measures categorised here as preventive is to ensure that attacks on components of the system will be thwarted before a fraudulent transaction can be executed. Detection measures are those taken to alert the issuer or system operator to an occurrence of fraud and to identify the source of the fraud. Containment measures are intended to limit the extent of any fraud once it has been committed. Of course, measures to detect and contain fraud may also have an important deterrent function and thus serve to prevent fraud as well. In addition, certain security measures, notably cryptographic techniques, are critical to the security of electronic money products throughout the stages of prevention, detection and containment.

4.1 Prevention measures

4.1.1 Tamper-resistance of devices

The electronic devices used in electronic money products provide the first line of defence against outside attacks. In card-based systems, security-related processing is performed inside a physically secured module, such as a smart card containing a microprocessor chip. The merchant's secured device might also be a smart card or what is sometimes referred to as a secure application module (SAM), a secure computer component integrated into the merchant's payment-processing terminal.

---

[7] In practice, the potential for repudiation of transactions is not unique to electronic money products, and has not been a major source of fraud in existing payment instruments compared with theft and counterfeiting.

[8] In a number of cases, electronic money product developers have not implemented the full range of security measures in pilot programmes, but state that they intend to do so at the time of more widespread introduction of their products.

Annex 5 provides additional information on smart cards and their security features. Tamper-resistant features of these cards are aimed at protecting the data and software from unauthorised observation or alteration. These highly sophisticated features include both logical (software) and physical (hardware) protection. The software code itself resides in the chip and is designed to be protected from any external observation or modification. Software protection includes features of the application and operating system that prevent data stored in memory from being accessed or changed except according to predefined authorisation and access protocols, often involving cryptographic techniques, as discussed below.

Data storage areas within smart cards contain different levels of security. Typically, any data that will not be altered during the life of the card are stored in read-only memory (ROM) during the manufacturing process. Sensitive but alterable data are stored in the EEPROM (electronically erasable programmable read-only memory) portion of the memory, which can be changed by the chip's internal functions.

Hardware protection is created during the manufacturing process and includes physical barriers that prevent optical or electrical reading or physical alteration of the chip's contents. Size, in terms of the width of the chip's wiring, is an important physical barrier for microchip cards. The smaller the wiring, the more difficult it is to probe physically the contents of a chip without highly specialised and expensive equipment. Physical barriers also include external coatings as well as multiple layers of internal wiring that are very difficult to remove without damaging the chip itself. Active tamper-resistant features include sensors within the chip that detect unusual levels of heat, light and electrical current and render the chip inoperable under an attempted attack, as well as providing evidence that tampering has been attempted ("tamper-evident"). Other design features reduce the usefulness of data gathered through unauthorised probing of the chip. For example, the layout of the components of the chip, as well as sensitive data such as cryptographic keys, are physically scattered throughout the chip.

These hardware protection features would very probably prevent the contents of a single chip from being successfully analysed or "reverse-engineered" even by a sophisticated attacker. However, if legitimate chips are widely available, attackers could attempt to piece together information from attacks on multiple chips; moreover, the success rate in analysing chips for fraudulent purposes could be improved through repeated attempts on a number of chips. Such attacks would be feasible for microchip manufacturers or organisations that reverse-engineer computer chips on a commercial basis.

In software-based electronic money systems, by definition, there is no physical protection built into the product itself that would prevent the user or an outside attacker from observing or tampering with the data or software used in the system. The software itself typically contains access control mechanisms to prevent the user from changing or duplicating data in an unauthorised manner. Software protection would typically deter only unsophisticated users, however, as software designed for use on standard personal computers can be altered using readily available programming tools.

4.1.2 Cryptography

Cryptography is one of the most important components of fraud prevention in all electronic money systems examined by the Task Force.[9] The subject of cryptography is highly complex and is covered in more detail in Annex 7.

---

[9] A number of countries have laws regulating the use or export of cryptographic software or hardware. The Task Force did not address these issues, as they may involve questions of legal interpretation and were not cited as major obstacles to security design by suppliers of electronic money products. However, such laws may have implications for some electronic money products depending on the countries where the products are manufactured and used and on their design.

Purposes of cryptography. Cryptographic techniques provide the logical protection of electronic money systems by ensuring the confidentiality, authenticity and integrity of devices, data and communications used in transactions. There are a number of different cryptographic techniques that are used for different purposes in electronic money systems.

Encryption is a technique used to protect the confidentiality of data during transmission or while stored on a device. Encryption is particularly important for certain types of sensitive data used in security processes, such as cryptographic keys. Other information, such as payment amounts or card serial numbers, may not necessarily be transmitted or stored in encrypted form.

Cryptography is also commonly used in electronic money products to authenticate the identity and privileges of devices in transactions. Before a device will respond to commands issued from another device, it will perform cryptographic challenges; only a device with the appropriate cryptographic keys will produce the correct responses. For example, critical control data, such as the maximum balance on the device, are generally protected against alteration except by devices holding cryptographic keys maintained by an issuer or central system operator. Digital signatures are one means of authenticating the identity of a device that sends a particular message and may also be used to prevent fraudulent repudiation of transactions.[10]

Cryptography is also used in some systems to certify the validity of electronic notes or other data created by an issuer or system operator. The security of note-based (or cheque-based) systems depends at least partially on cryptographic protection of the electronic note itself, which is typically certified by a digital signature created by the issuer's device or system. This approach is common in software-based systems, in which balances cannot be protected physically but can be protected mathematically.

Cryptography is commonly used for verifying the integrity of messages exchanged between devices in electronic money systems, that is, detecting whether or not a message has been altered before reaching its intended recipient. Message authentication codes may be used for this purpose. Creation of a fraudulent message that is successfully received as a valid message would require knowledge of cryptographic keys. Cryptographic techniques can also be used to protect the integrity of software transmitted over open networks.

Types and strength of cryptography. Cryptographic techniques rely on mathematical algorithms together with parameters known as keys. Many different cryptographic algorithms are available. Algorithms are usually classified into symmetric key and asymmetric (or public) key cryptographic systems. Symmetric algorithms require devices to use the same secret cryptographic key for encrypting and decrypting messages. The most commonly known symmetric key algorithm is Data Encryption Standard (DES), which has been adopted as a standard in many countries, particularly in the financial services industry. The DES algorithm can be used in a process that greatly increases its strength, known as triple-DES, whereby three separate encryption and decryption operations are performed using a double-length DES key.

Asymmetric algorithms allow the use of a combination of private and public keys in the encryption and decryption processes. A message encrypted with a public key can only be decrypted by its private key counterpart. Similarly, only a message encrypted with a private key can be decrypted with the public key counterpart. While the public key may not need to be protected from outside observation, the private key is stored only on the user's device, thus limiting its vulnerability to attack. The design of algorithms is such that, in the current state of mathematics, calculating the private key from the public key is practically infeasible. RSA is one well-known asymmetric cryptographic algorithm, although others are also used.

Systems using cryptography can be attacked by exploiting weaknesses in the algorithm, by stealing secret keys, or by testing all possible keys in turn ("brute-force attacks"). For a given

---

[10] Whether or not digital signatures are adequate to ensure that a payment has been legally authorised may involve additional technical as well as legal issues which the Task Force considered to be outside its scope.

cryptographic algorithm, the longer the key, the more difficult and costly it is for an attacker to derive the keys or encrypted information through a brute-force attack.[11] However, longer keys also increase processing times, which may be a constraining factor for current generations of IC cards. The strength of the algorithm itself is usually verified mathematically and through repeated testing.

The card-based electronic money systems investigated by the Task Force use (or plan to use) both symmetric and asymmetric cryptography. The most common algorithms used in electronic money products are DES and triple-DES algorithms, so-called "hash functions", and RSA or other asymmetric algorithms. Asymmetric key lengths range from 512 bits to 2,048 bits. The Task Force found that most suppliers of electronic money systems have made similar assessments regarding the strength of particular encryption algorithms, necessary key lengths for symmetric and asymmetric algorithms and good key-management practices. Most are using or plan to use published cryptographic algorithms that have been subject to extensive testing.

The use of "active" or "dynamic" asymmetric cryptography, in which chip cards generate digital signatures or perform other cryptographic calculations, can be applied to prevent attacks that may be attempted through replaying previous messages and observing the exchange of cryptographic information. Active asymmetric cryptography, however, requires more powerful microprocessors (known as crypto-processors), which are currently more costly to produce, and may result in slower transaction speed and reduced reliability of devices, according to suppliers. Thus, at this stage of their implementation, many products rely on the use of "passive" asymmetric cryptographic certificates stored on each card, together with dynamic symmetric cryptography, in which unique "session" keys are generated for each transaction, as discussed in Annex 7. However, note-based or cheque-based products generally utilise active asymmetric cryptography.

Systems using cryptography can also be attacked through weaknesses in their implementation. For example, the software that performs cryptographic functions must be properly designed and implemented, and any use of random data to generate keys must be truly random or patterns could be recognised that would aid in a brute-force attack. Extensive testing of the product is the most effective means of correcting such implementation weaknesses.[12]

Key management and storage. The key management of a system comprises the different types of cryptographic keys and their relationship, generation, use, distribution, storage and validity. Decisions in this area are critical to the security of the product as a whole.[13] Damage to a system through the compromising of cryptographic keys may be reduced by limiting the use of each key. Many electronic money systems contain different keys that provide access to different functions, such as load, purchase and deposit functions. Individual cards may each store a unique key, derived from a master key. Highly sensitive load keys that allow the increase of balances on a card are generally held only by the issuing institution and may involve longer key lengths. The ability to change cryptographic keys or algorithms used in the system quickly is a security measure envisioned by many electronic money systems. Suppliers interviewed by the Task Force indicated that they anticipated a relatively short key life cycle, sometimes a matter of months for critical keys.

All electronic money systems involve cryptographic keys that must be kept secret, or secure against unauthorised observation, in order to prevent unauthorised duplication or alteration of data. In card-based systems, various security measures have been developed to safeguard keys in storage on devices and in transmission between devices. For software-based systems, in particular

---

[11] Comparisons of key lengths across different algorithms are not always meaningful; for example, asymmetric cryptographic algorithms typically require much longer keys than symmetric algorithms in common applications.

[12] For example, such weaknesses have been uncovered and publicised in certain network access software following widespread market introduction.

[13] As discussed in Annex 6, certain international standards for payment systems provide guidance on desirable key-management practices.

those that involve access to open computer networks, storage of cryptographic keys poses greater challenges, because the user's device cannot be assumed to be secure with any degree of certainty.

Certification authorities (CAs) may be necessary for systems employing asymmetric cryptography. CAs are typically centralised databases that certify, store and distribute public keys and information identifying the holder of the corresponding private key. Owing to their limited use of active asymmetric cryptography, most electronic money systems examined by the Task Force provide their own CA facilities. Those that require widespread, routine distribution of public keys for each user face greater challenges. In either case, the compromising of a CA would be a significant threat to an electronic money system. In particular, the use of third-party CAs or multiple CAs (for example within an international system) raises a number of security issues that may require further analysis if they are ultimately implemented in electronic money systems.

4.1.3 Online authorisation

In card-based systems, online authorisation by the issuer is typically only required at the time the device is loaded by a debit to a bank account. Such authorisation is required, as in a standard ATM transaction, to ensure that the holder of the card is authorised to access funds in a particular account. A standard personal identification number (PIN) is usually required of the consumer in such transactions. The deposit or collection function between merchants and their acquirer also typically occurs in an online manner. Centralised systems at the acquirer verify merchant transaction logs to ensure that no transactions have been transmitted more than once. In some card-based systems, the merchant terminal might request an online authorisation for a purchase transaction; this could be done randomly or on the basis of certain card or transaction parameters.

Online authorisation is generally considered to be necessary for all transactions in software-based electronic money products.[14] In order to deter a user or outside attacker from copying a particular electronic note and "spending" it several times over, a central authority must verify each transaction sequentially on the basis of information about notes that have previously been issued and redeemed. Such methods would not necessarily prevent fraud, however, but might only detect it after the event. In some systems, the use of sophisticated cryptographic techniques would enable the issuer to determine which party instigated the fraudulent transaction.

4.1.4 Other measures

Electronic money systems may provide additional levels of security against fraud as well as malfunctions by requiring individual devices to perform additional verifications during transactions. These could include, for example, verifying expiration dates, numbers of transactions executed with the device, balances on the device (against its maximum balance) and the maximum balance itself.

Electronic money systems also include measures to prevent the creation of unauthorised balances through interruption of transactions. Message protocols are designed so that transactions are completed only if all messages defined for that transaction have been successfully exchanged. Incomplete transfers, such as those caused by interruption of power supply or of messages, can at worst lead to the debiting of amounts on one device without their being credited to the counterpart device. Logs of incomplete transactions are typically stored on the devices for future reference or investigation by the issuer or system operator.

Finally, procedural and administrative controls provide important safeguards against attempted fraud. Tasks such as card manufacture, cryptographic key management and card personalisation are subject to strict access controls and are separated geographically and

---

[14] Even the use of asymmetric cryptography by the consumer, merchant and issuer may not be sufficient if users' private keys are stored on a standard personal computer rather than a specialised hardware device.

administratively, increasing the number of employees that would need to collude in order to gain enough information to compromise system security. Terminals, particularly those that allow loading of balances, are distributed in a controlled manner, and may be supervised through remote monitoring by a central operator. Control over the merchant environment may also play an important role in security administration, as merchant terminals may have higher balance limits and be an attractive entry point for an outside attacker. Administrative controls are also necessary to prevent the possibility of fraudulent issuance of electronic money by an issuer or its employees.

4.2 Detection measures

4.2.1 Transaction traceability and monitoring

Individual electronic money transactions, once executed, are subject to a variety of different security-related monitoring and verification procedures. In most of the card-based systems analysed, each transaction can be identified by a unique number, based on the card's serial number and its transaction counter, which increases by one increment for each attempted transaction. In the case of note-based systems, each note has a unique serial number.

The frequency, location and extent of monitoring of transaction-specific information by a central operator varies across systems and may be conducted at the option of the operator according to the particular environment. In some systems, transaction information, including the identity of both devices in the transaction, is transmitted to the central point some time after the transaction has taken place. Typically, such transmission by merchants is required within a specified time-frame. For unattended terminals, such as vending machines, this process might occur up to two weeks after the transaction date. In most systems, the devices themselves, including those held by consumers, store a full or limited record of transactions performed. This record could be read at a later time by a central system. Some systems truncate information at the level of the merchant or acquirer. Some systems verify every transaction that is executed; this is clearly quite costly to perform. Other systems check transactions on an ad hoc basis or in response to evidence of suspicious behaviour.

Transactions can be subject to financial verification as well as security verification. Financial verification may involve accumulating transaction amounts for each device and calculating "shadow balances" for devices, which are stored in a central database. Although the exact balance on each device at any point in time cannot be calculated with complete accuracy owing to the time-lags in clearing transactions, transactions made with a particular card can be compared against the shadow balance maintained for that card to ensure that it is not inconsistent with the prior transaction data. This type of active transaction monitoring provides a very high degree of certainty that any fraudulent transactions or alteration of balances on a card will be detected at some point, although the time that may elapse before such detection could vary considerably depending on the design of the particular system. Some electronic money systems examined by the Task Force do not check every transaction against a centrally held balance, either because not all transaction data are routinely collected or for cost reasons.

Security verification by the issuer or central operator involves verifying message authentication codes, transaction sequence numbers, information about previous payment and load transactions and other information contained in transactions or stored on devices. In note-based systems, as mentioned earlier, serial numbers of notes used in transactions can be verified against a central list. Some verification of cryptographic information may be performed at the central operator or issuer level, using cryptographic keys that are not contained in merchant terminals. This provides an added level of security against the compromising of a merchant terminal.

To the extent that greater transferability between users limits information collected by a central point, it reduces the effectiveness of transaction monitoring. However, the Task Force did observe note-based or cheque-based systems that permit transferability within certain parameters but also collect a full transaction log of each transfer attached to each "note" for later monitoring by the

issuer. Thus, transferability and strong traceability and detection measures are not necessarily mutually exclusive but depend on the logical design of the product.

4.2.2 Interaction with a central system

Online interaction with the issuer or central operator of an electronic money system is a commonly used security feature of card-based systems. Such interaction allows the central operator to check security parameters on the card for consistency, to update security measures on the device, such as cryptographic keys, and, in some cases, to gather additional transaction data from the device. The transaction log and records of any errors or incomplete transactions can be read and stored by the central system. Such measures increase the probability that any attempted fraud will be detected within a short period.

Events that may require interaction with the central system include routine load or deposit transactions, resolution of failed transactions or multiple failed attempts to enter a PIN. In addition, the expiration date of the device or of balances or notes stored on the device could also trigger online interaction. In some systems, or as planned future enhancements, the device itself will automatically cease functioning after a certain number of consecutive offline transactions, thus requiring online interaction. Of course, some of these measures could reduce convenience and flexibility for the holder.

4.2.3 Limits on transferability

Limits placed on the transferability of stored-value balances or notes may reduce the opportunities for fraudulent balances to be used without detection. If balances on devices are transferable to other users without information being made available to a central point, the origin of any fraudulent balances may be more easily disguised. In most systems reviewed by the Task Force, consumers are only permitted to make transfers to merchant terminals or to issuers; there is no provision for consumer-to-consumer transfers. Consumers might be permitted to transfer balances to an "affiliated" device, such as one held by another member of their family, but not to unaffiliated devices. Other systems may permit consumer-to-consumer transfers at an ATM or other terminal with an online connection to the issuer or other central system. Certain types of device may be permitted to make transfers only to other devices with certain parameters. For example, to deter attempts at merchant fraud, merchant terminals may be permitted only to transfer balances to individual acquiring institutions.

Even those systems that permit consumer-to-consumer payments may include some limitations that can help detect attempted fraud. As noted earlier, devices could be designed to require interaction with a central operator periodically, so that consumer-to-consumer transaction records stored on the device could be checked. Software-based systems that permit transferability typically operate online; thus each transaction effectively requires interaction with the central operator.

4.2.4 Statistical analysis

Electronic money systems can also implement procedures to analyse system-level data on payment flows in order to detect unusual volumes of payments that could be indicative of fraud. Issuers or a central system may utilise the automated procedures for pattern recognition that have become common in the credit card industry to detect abnormal activity, such as those using artificial intelligence and neural network techniques. At the highest level, the system can track the volume of balances issued and redeemed each day; any level of redemption outside the norm could trigger more detailed investigations. For example, the volume of payments collected by merchants can be analysed by comparison with other merchants of the same type or with normal daily payment volumes.

Statistical analysis procedures require the accumulation of a large database covering normal payment activity over a given period. These data could be analysed for unusual payment patterns, taking into account seasonal patterns and differences across geographic locations, for example. It is not clear, at this stage, how effective a tool statistical analysis will become for detecting specific instances of fraud, or how difficult it would be for sophisticated attackers to disguise their activity within these normal payment patterns.

4.3 Containment measures

4.3.1 Time and value limits on devices

Limits on the size of balances permitted to be stored on consumer and merchant devices are a very important security feature of electronic money systems. Note-based systems may not contain a direct value limit but in some cases may limit the number and denomination of notes issued to a particular device at any given time. While the direct effect of value limits is to contain the magnitude of losses from successful fraud attempts, the indirect preventive result may be equally important - to deter attempted fraud by reducing the potential financial gain. Any attacker would need to duplicate or alter a large number of devices to make the effort financially worthwhile. Of course, the effectiveness of balance limits relies on highly secure means of storing the maximum balance limits to prevent tampering as well as on routine verification of the actual balance against the maximum balance permitted. Moreover, limits on consumer devices may not help contain breaches of security of higher-balance merchant terminals.

Expiration dates on devices and on value also serve to contain the extent of any fraud, as a fraudulently altered device would only be usable for a limited period. Importantly, such measures may also be used to force the user to interact with the central system, where fraud could be more easily detected. In card-based systems, devices may contain limits on the maximum number of transactions that a particular device can perform.

4.3.2 Registration of devices

Registration of the identity and address of the holders of devices with the issuer or central authority would facilitate investigation of any attempted fraudulent activity. In many of the electronic money systems analysed, both consumer and merchant devices are required to be associated with specific bank accounts, from which funds can be withdrawn in loading transactions. Anonymous purchases of cards, for example at vending machines in exchange for currency, so far appear to be the exception rather than the norm; moreover, functional limitations could be placed on such devices compared with those that are individually registered. In software-based systems, users would be required to register their identity with issuers in order to transfer funds into or out of the systems, as well as to receive software and register cryptographic keys and other information necessary to execute transactions.

Registration of merchant devices may be particularly important. Because merchant devices may have much higher balance limits than consumer devices, control over distribution of and access to these terminals is a necessary security measure. The same holds true for devices held by entities distributing or collecting stored-value balances.

4.3.3 Hot lists and disabling of devices

Hot lists are records of the serial numbers of suspect devices maintained by a central system operator. These lists are used to check for suspect cards at each point of interaction with the central system, and can cause the cards to be disabled or retained by a terminal. In some cases, hot lists can also be distributed to merchant terminals to prevent purchases by suspected devices or

devices within a certain range of card serial numbers. The hot lists held on merchant terminals can be updated when the terminal makes an online connection to the system operator. Owing to cost considerations, most suppliers interviewed envision using this capability only for fraudulent devices, rather than to block lost or stolen cards at the merchant level. In software-based systems in which devices would not be identified by their serial numbers, it may be more difficult to identify users suspected of fraudulent activity and prevent them from operated devices, although this will depend on the manner in which users are registered or otherwise identified in the system.

Other measures that cause automatic disabling of devices can include multiple attempts to enter a PIN or multiple failed transactions. In some electronic money products, a PIN can be used to "lock" the device in order to discourage theft by preventing use by an unauthorised person.

4.3.4 System suspension

Many of the electronic money systems plan to implement facilities to rapidly change the cryptographic keys or algorithms used if a wide-ranging fraud is detected or suspected. A longer-term measure would be to replace cards or software if it were suspected that the design was compromised. Ultimately, in the face of widespread fraud, system operators could resort to the extreme solution of disabling all terminals and recalling devices.[15] Given that some transactions typically take place offline, and that some time would be needed in order to notify participants, complete closure probably could not take place immediately and thus would not fully contain losses.

5. EVALUATION OF SECURITY MEASURES

5.1 General assessment

The overall impression gained by the Task Force was that measures are available to provide adequate security for electronic money systems, in particular compared with other common forms of retail payment. However, there are a number of challenges to developers in terms of implementation. While the security architectures of most electronic money systems share many common design features, a wide range of options are available to product developers in terms of specific chip card security measures, cryptographic algorithms, key lengths and transaction monitoring. These options present trade-offs for product developers in the areas of cost, functionality, speed and reliability. The degree of emphasis on these other considerations will have important implications for the level of security ultimately chosen.

Security measures for electronic money products are highly complex. There is no single security measure or set of measures that can be said to be sufficient for a particular product. As discussed in Annex 6, international standards have been developed for particular aspects of electronic money products, such as the basic functionality of chip cards, certain cryptographic techniques and communication protocols, but these standards in themselves are not sufficient to ensure adequate security for a product as a whole. In addition, the development of standards may naturally tend to lag behind technological advances, especially in areas of rapidly changing technology. It is the combination of measures, together with the rigour with which they are implemented, that will serve to reduce risk most effectively. Thus, it is more important to focus on the overall security risk management approach for a particular product, rather than on the use of individual measures. In addition, relatively low maximum balance limits on devices may represent one of the simplest yet most effective deterrents to fraudulent attacks.

---

[15] Of course, suspending the system could have important financial repercussions for consumers and merchants; these are not discussed here.

Compared with other forms of payment that are paper-based or rely on plastic cards with magnetic stripes, it is widely accepted that microchip cards are much more difficult to counterfeit or fraudulently alter.[16] In addition, maximum amounts that could be held on devices in most proposed systems are generally lower than the amounts at risk for most debit or credit cards. However, security measures at each level of an electronic money system (e.g. consumers, merchants, financial institutions) should be commensurate with the degree of risk at that level. For example, merchant devices could hold significantly greater amounts and thus may be a more likely target for attack; additional hardware protection and other controls may therefore be desirable for higher-value merchant devices. Data and devices held at issuers would be particularly sensitive and would most probably be subject to the highest level of security.

5.2 Specific security measures

Physical barriers against tampering with devices provide one of the most important security measures for electronic money products. The cost and resources necessary to physically alter or reproduce the various types of microchip cards are fairly well known by industry experts. Tampering with microprocessor cards is beyond the means of the casual criminal, while even for experienced or professional computer thieves, tampering with chip cards would also be extremely difficult and costly.[17]

However, with legitimate electronic money devices widely available in the market, criminal organisations will be able to continually improve their methods of attack, even if initial attacks on a chip card fail. Thus, it can be assumed that even the most sophisticated tamper-resistant features may eventually be breached, potentially permitting analysis and reproduction of the contents of the device. As a result, continual strengthening of the tamper-resistant features of card-based products will probably be necessary.

For software-based products, data stored on the devices used by consumers and merchants can be expected to be copied or otherwise compromised by only moderately sophisticated attackers. The software itself can be reverse-engineered and examined closely for vulnerabilities, a process which is generally much more difficult when the software is physically protected on a chip card. As a result, software-based systems must generally rely on other measures such as online, real-time authorisation.

Published cryptographic algorithms that have been widely tested and in use for a considerable amount of time provide a high level of security; products should not rely on the secrecy of the algorithm for protection. In addition, longer key lengths greatly increase the cost and time for a brute-force cryptographic attack. RSA keys are generally at least 512 bits in length; in fact, 768 bit keys are now becoming common and some keys are as long as 2,048 bits. Key-management techniques such as separation and diversification of cryptographic keys, both across functions and across devices, help to contain any losses resulting from the keys on a single device being compromised. Longer keys may be used for more sensitive functions, such as those performed by issuers.

---

[16] It is difficult to assess the cost of counterfeiting electronic money products compared with physical currency, given the recent technological advances in currency production, such as the incorporation of holograms and the use of specialised materials. It is well known that the cost of counterfeiting magnetic stripe cards is quite low.

[17] While several incidents of counterfeiting or tampering with memory chip cards have been reported in Europe, counterfeiting of microprocessor cards is considered to be significantly more difficult. Non-financial applications of microprocessor cards may involve less advanced security features owing to the lower financial risks that could result from the cards being compromised. There have been no reports thus far of IC chips used in general-purpose stored-value cards being compromised by an outside attacker.

The feature of transferability between users found in some electronic money systems does not, in itself, pose greater security threats; products have been developed that provide transferability while still permitting full traceability of transactions. Shadow-balance accounting should provide a very high degree of detection of possible fraud, provided that transactions are required to be cleared within a fairly short time-frame. Systems that do not rely on shadow-balance accounting, either for cost reasons or because transferability features make the collection of data difficult, must rely on other measures to ensure a high level of security, such as highly tamper-resistant chips, strong cryptography, more extensive security verification between devices, relatively low balance limits and more frequent online interaction with a system operator or issuer. Statistical analysis of payment patterns may help to detect suspicious activity, but the effectiveness of such techniques has not been proven. Such monitoring might raise the cost of attempting fraud, because activity would need to be more carefully disguised.

The use of an insecure network, such as the Internet, for transmitting payment messages does not in itself create additional security hurdles.[18] All electronic money products operate via messages exchanged between devices, and it is possible to observe or intercept these messages whether they flow over a computer network or through more direct means, without the knowledge of one or both of the parties to the transaction. Electronic money products are therefore designed on the assumption that messages are not transmitted over a secure medium.

Finally, as with other payment systems, administrative and procedural controls over development and operation are critically important security measures. Given the advanced technology used in electronic money products, administrative channels can be expected to be the least costly method of attacking a product, and should therefore be addressed through administrative security control measures.

5.3 Industry assessment

Electronic money products have been developed by organisations with varied experience. The Task Force found that the particular background and experience of different suppliers is evident in their approach to security design. Some systems have been developed by large organisations or banking associations with long experience in operating payment systems. Some would utilise existing payment infrastructures, such as credit or debit card networks, for the operation of their products; these networks typically already address technical security management procedures. New entrants to the payment systems arena may have advantages in terms of flexibility, costs and innovation, but may have less expertise in managing security risks. In particular, because software-based products require less costly physical infrastructure, they may be introduced by organisations less experienced in operating payment systems.

Developers of electronic money products have invested considerable resources in designing and assessing the security features of their products, as well as in analysing the impact of cost and functionality considerations on security. While suppliers interviewed by the Task Force have clearly focused considerable attention on the technical security of their products, security assessments conducted thus far have in most cases been partial evaluations of specific components of a product, rather than comprehensive security risk assessments of the entire system. Comprehensive security assessments are complex, lengthy and expensive to conduct. Owing to the complexity and evolutionary nature of the technical security aspects of electronic money products, it may be difficult for one organisation to perform such a comprehensive assessment. Moreover, there are few organisations qualified to perform such evaluations. A comprehensive security assessment must balance the benefits of an integrated, comprehensive risk-management process against the risks inherent in concentrating detailed security information in any one organisation. However, the Task

---

[18] Use of the Internet does, however, provide a lower-cost channel for outside attacks on computers connected to it, although these issues are not addressed in this report.

Force concluded that such assessments conducted by objective, independent experts within an overall security policy framework would serve to significantly enhance confidence in the security of the product.

5.4 Current status and future developments

The Task Force observed that current pilot projects, such as those for stored-value cards in a number of countries, are generally designed to test the business case for electronic money products rather than the specific security implementation. It can be expected that there will be significant changes to the security architecture of these products over the next few years as they are introduced to a wider market. In particular, many suppliers indicated that they are upgrading the physical security and processing power of microchips used in electronic money products, as well as moving to the use of asymmetric cryptography. Suppliers also plan to increase the length of cryptographic keys to provide additional security, and to change keys and security procedures periodically in order to increase the cost of attacking their systems.[19]

Cryptographic techniques and chip card technology are constantly evolving. New means of attack will certainly also be developed and the costs of mounting such attacks will decline as specialised equipment becomes more widely available. As a result, electronic money systems will face challenges in ensuring that their systems can be regularly upgraded and modified to meet new security threats. In the area of cryptography, continuing increases in computing speed should work to the advantage of electronic money suppliers, as cryptographic keys can be lengthened fairly easily, greatly increasing the cost of successful cryptographic attacks.

The cost of these measures, in particular the cost of producing powerful and highly tamper-resistant chip cards, is likely to be a major factor in the implementation of card-based electronic money systems for the foreseeable future. It is unclear how the development of international standards and features permitting interoperability of products will contribute to the security of electronic money products. In addition, products providing for multiple applications housed on one device may raise security issues that may not have been fully addressed at this stage, given that such products have not yet been introduced.

At this stage, software-based stored-value systems, particularly those designed for use on the Internet, are not well developed from a commercial perspective, and the Task Force was thus unable to examine the likely implementation features of such systems that are critical to their security. Software-based products providing access to traditional credit card or bank accounts are much closer to commercial implementation, however, but were not the focus of the Task Force's analysis; industry security standards in this area are also close to completion. In general, suppliers indicated that payment systems designed for use over computer networks may move towards use of tamper-resistant devices in the future, for example smart cards that would perform security-related functions for the consumer. Additional security assessments in this area may therefore be useful in due course. These risks deserve additional investigation, in particular as new techniques and potential industry standards for protecting information transmitted over the Internet come to be introduced.

---

[19] For example, 40 bit DES keys have been standard for many years, but are now considered to be vulnerable to attack; the stronger triple-DES algorithm is preferable even for systems using 56 bit DES keys.

6. OTHER CONSIDERATIONS

6.1 Use for criminal activities

Some characteristics of certain electronic money products, such as their relative lack of physical bulk, their potential anonymity and the possibility of effecting fast, remote transfers, might make them more susceptible than traditional payment systems to criminal activities, in particular money laundering. The Task Force's investigation of electronic money products has shown that, in most cases, the security features that suppliers intend to implement in order to protect issuers from fraud risks might make these products less attractive for use in criminal activities than many existing payment instruments.

For example, events that trigger a required interaction with the central system increase the chance that suspicious activity will be recorded and potentially made available to law enforcement agencies. In all card-based systems examined by the Task Force, devices have unique serial numbers. In most cases, transactions can be uniquely identified by a transaction number, and transaction logs of some kind are stored on devices themselves, and in many cases on a central database as well. Limits on transferability and expiration dates on devices or balances also constitute practical obstacles to the extensive use of these products for money laundering. Risk control procedures based on statistical analysis may also help detect criminal behaviour.

Products that do not require registration of the user with an issuer or other central authority, such as those that can be purchased at vending machines, are typically planned to have quite low limits on values and might not be reloadable. Even for software-based systems that permit remote payments in which the sender may not be identified, users must register with the issuer in order to deposit funds for use in the system and to register cryptographic keys. Given these limits, successful money laundering would be likely to require some degree of involvement or collusion by a financial institution participating in the system. Such activities may be more feasible in certain types of electronic money system if they permit large-value payments to financial institutions in remote locations, such as via the Internet, as well as unrestricted and unmonitored participation by institutions anywhere in the world; these features may depend upon the actual implementation of particular systems.

6.2 Reliability

Reliability encompasses the robustness of devices and networks and timeliness of transactions in electronic money systems in the face of malfunctions, system interruption and transmission failures or delays. The failure rate of chip cards is routinely analysed and documented by electronic money suppliers and chip card manufacturers. Card manufacturers may guarantee a certain level of reliability in terms of card life and the number of transactions that can typically be performed. To the extent that a central system is used for online authorisation, clearing of transactions, storage of cryptographic keys or other critical functions, contingency arrangements for such systems would be an important factor in ensuring reliability.

Developers have implemented measures to address the impact on reliability of interrupted messages due to communications or electrical failures. In some cases, users might be required to return to the issuer to reactivate the device. Reliability of the network in terms of speed and message integrity is likely to be a significant factor in use of the Internet for transmitting payment-related messages, particularly for those systems that operate online. Systems that utilise the Internet or other remote communications methods must ensure that transaction protocols are particularly resilient to delayed or interrupted transactions.

6.3 Privacy

Advanced cryptographic techniques offer the potential for a greater degree of privacy in financial transactions than has been possible with other types of electronic payment. However, proposed electronic money products differ greatly in the degree of privacy they would provide to consumers. For example, some electronic money systems would permit users to transfer electronic notes certified through cryptographic algorithms by the issuing institution without revealing the identity of the sender. Other systems would allow consumers to purchase devices with balances stored on them without revealing their identity, for example at vending machines.

Most of the electronic money systems examined by the Task Force would prevent unauthorised access to transaction information by outside parties, as the consumer's identity would not be contained in transaction messages, and in some cases these messages would be transmitted in encrypted form. Moreover, merchants generally would not have access to information on the identity of the user in a transaction; their devices would record the serial number of the consumer's device but they would have no way of associating that device with an individual. However, a cardholder might voluntarily provide personal information in order to participate in a loyalty or discount programme at a particular merchant.

The anonymity of transactions vis-à-vis the central operator or issuer depends on factors such as the logical design of the system (note-based or balance-based), the degree of truncation of payment messages and whether holders or devices are registered with issuers. If full transaction information is transmitted to the central point, the issuer will probably be able to relate transactions to particular consumers fairly easily; this could reduce the level of consumer privacy compared with certain traditional payment methods. Some suppliers have stated that they intend to retain such detailed transaction information but make it available only for law enforcement purposes.

7. CONCLUSION

Electronic money products have the potential to provide important benefits to payment systems if implemented with due regard for security. The Task Force concluded that no system can be made fully secure against all types of attack. Determining the appropriate level of security for a particular product should involve consideration of the magnitude of potential risks, the cost of implementing varying levels of security, the impact on the functionality of the product and the implications for privacy.

In its interviews with suppliers, the Task Force was impressed with the amount of research that has been undertaken and resources that have been expended on the security of electronic money products. Many sophisticated security measures have been developed that should provide a high degree of security for electronic money products in their initial stages. However, risks may arise in the implementation of these measures. Thus, each product must be evaluated on its own merits. Moreover, it can be expected that there will be significant changes to the security architecture of these products over the next few years, as the resources and capabilities available to both suppliers and potential attackers of these systems increase.

Owing to the technical complexity of these products and the high level of scientific expertise required to assess many aspects of security, it may be difficult for one organisation to evaluate objectively and comprehensively the security of an entire product. The Task Force concluded that an integrated, overall risk-management approach to security, including independent security assessments, is an important component of the security of these new products.

ANNEX 1

Glossary

Acquirer: in an electronic money system, the entity or entities (typically banks) that hold deposit accounts for merchants and to which transaction data are transmitted.

Asymmetric cryptography (also called public key cryptography): a set of cryptographic techniques in which two different keys (private and public keys) are used for encrypting and decrypting data. The private key is kept secret by its holder while the public key is made available to communicating entities.

Audit trail: a sequential record of events having occurred in a system.

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

Availability: the ability of services and information to be accessed by users when requested.

Balance-based system: an electronic money system in which the electronic funds are stored on a device as a numeric ledger, with transactions performed as debits or credits to a balance.

Biometric: refers to a method of identifying the holder of a device by measuring a unique physical characteristic of the holder, e.g. by fingerprint matching, voice recognition or retinal scan.

Bit: the basic data element: a binary digit, either 0 or 1.

Brute-force attack: a method of cryptanalysis in which every possible cryptographic key is tried.

Byte: a series of 8 bits.

Certification authority: an entity entrusted with creating and assigning public key certificates.

Challenge-response: a means of authentication in which one device replies in a predetermined way to a challenge from another device, thus proving its authenticity.

Ciphertext: the encrypted form of data.

Closed network: a telecommunications network that is used for a specific purpose, such as a payment system, and to which access is restricted.

Confidentiality: the quality of being protected against unauthorised disclosure.

Contact cards: cards that require physical contact through an electronic connection surface between the card and the card reader or terminal device.

Contactless cards: cards that do not require physical contact between the card and the card reader or terminal.

CPU (Central Processing Unit): area of a computer system (and of an IC card) that performs computations.

Cryptanalysis: area of cryptography dedicated to studying and developing methods by which, without prior knowledge of the cryptographic key, plaintext may be deduced from ciphertext.

Cryptographic algorithm: a mathematical function used in combination with a key that is applied to data to ensure confidentiality, data integrity and/or authentication. Also called cipher.

Cryptography: the application of mathematical theory to develop techniques and algorithms that can be applied to data to ensure goals such as confidentiality, data integrity and/or authentication.

Derived key: a cryptographic key that is obtained by using an arithmetic function in combination with a master key and a unique identification value such as a card serial number.

DES (Data Encryption Standard): a symmetric cryptographic algorithm (ANSI standard) that is widely used, in particular in the financial industry. Triple-DES consists of operating three times on a set of data (encrypting-decrypting-encrypting) using a double-length DES key.

Digital signature: a string of data generated by a cryptographic method that is attached to a message to ensure its authenticity as well as to protect the recipient against repudiation by the sender.

Embedding: in IC card manufacturing, the process by which the chip module is mounted on the plastic carrier (card).

EEPROM (Electronically Erasable Programmable Read-Only Memory): the area of an IC chip used to store data. Data in EEPROM can be electronically erased and rewritten under the control of the operating system.

Electronic purse: typically an IC card containing an application that stores a record of funds available to be spent or otherwise used by the holder; the record of funds is updated as transactions are made. Additional funds may be added to the stored balance through a withdrawal from a bank account or by other means. Sometimes referred to also as a stored-value card.

Electronic wallet: a computer device used in some electronic money systems which can contain an IC card or in which IC cards can be inserted and which may perform more functions than an IC card.

Encryption: the use of cryptographic algorithms to encode clear text data (plaintext) into ciphertext to prevent unauthorised observation.

EPROM (Electronically Programmable Read-Only Memory): the area of an IC chip used to store data. Data in EPROM can only be written once and cannot be erased selectively.

Firewall: a hardware- and/or software-based system that is used as an interface between the Internet and a computer system to monitor and filter incoming and outgoing communications.

Fleckless: from the German "fleckenlos", which means spotless; a device (card) or a system is said to be fleckless when it can provide evidence that it has not been tampered with.

Hot list: in a card-based system, a list - held by the merchant terminal or other device - of suspicious card numbers or ranges of suspicious card numbers. The hot list is used to detect and to block any transaction with such cards.

IC Card (Integrated Circuit): a plastic card in which one or more integrated circuits are embedded. Also called chip card.

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

Internet: an open worldwide communication infrastructure consisting of interconnected computer networks and allowing access to remote information and the exchange of information between computers.

ISO (International Organization for Standardization): an international body whose members are national standards bodies and which approves, develops and publishes international standards.

Issuer: in a stored-value or similar prepaid electronic money system, the entity which receives payment in exchange for value distributed in the system and which is obligated to pay or redeem transactions or balances presented to it.

Key: a unique series of digits used in combination with a cryptographic algorithm.

Key length: the number of bits comprising an encryption key.

Key management: the design of the life cycle of keys and the relationships between keys which are used in a computer system for cryptographic purposes. Alternatively, when referring to a system in operation, the processes by which cryptographic keys used in a computer system are generated, stored and updated.

Load: the action of transferring electronic balance from an issuer to a consumer's device.

Master key: a cryptographic key, often used to generate other cryptographic keys.

Memory card: an IC card capable of storing information only.

Mask: the hardware specifications that define the physical and functional properties of the IC chip.

MAC (Message Authentication Code): a hash algorithm parametrised with a key to generate a number which is attached to the message and is used to authenticate it and to guarantee the integrity of the data transmitted.

Note-based system: an electronic money system in which the electronic funds are represented by records (electronic notes) that are uniquely identified by a serial number and are associated with a fixed, unchangeable denomination.

Offline: in electronic money systems, a transaction in which no direct connection is made between the device(s) involved in the transaction and a centralised computer system for the purpose of authenticating or otherwise authorising the transaction before it is executed.

One-way hash function: a mathematical algorithm (hash algorithm) applied to a message to generate a number that is attached to the message and is used to verify the integrity of the data transmitted. The result of the application of a hash function to a message is called a hash value.

Online: in electronic money systems, indicates that a direct connection is made to a centralised computer system for authorisation or validation before a transaction can be executed.

Open network: a telecommunications network to which access is not restricted.

Operating system: that part of the software of a computer system (including chips) that is closely tied to the hardware on which it runs and that performs basic input/output operations, computations, memory management, etc.

Personalisation: the phase of the IC card manufacturing process during which customer information is loaded into the card.

PIN (Personal Identification Number): a sequence of digits used to verify the identity of a device holder.

Plaintext: data which are not encrypted and are therefore in a readable form.

PCMCIA card (Personal Computer Media Control Interface Adapter): a device that is attached externally to a PC and that can perform various functions such as memory storage and modem communications. PCMCIA cards can be designed in such a way as to provide a certain level of tamper-resistance.

Prepaid card: a card on which is stored a record of funds available to the holder. Also used to refer to a card that provides its holder with access to a limited range of services (e.g. a telephone card) or goods which have been prepaid, even though the card itself does not store a record of funds.

Protocol: procedures for the interchange of electronic messages between communicating devices.

Privacy: in the context of a payment system, the fact that no information which might permit determination of behaviour may be collected without the consent of the individual to whom it relates.

Public key cryptography: see asymmetric cryptography.

RAM (Random-Access Memory): the volatile memory area of a chip that is used for calculations and can only store data when electrical current is being supplied.

Repudiation: the denial by one of the parties to a transaction of participation in all or part of that transaction or of the content of the communication.

Reverse-engineering: the process of analysing software code in order to determine how the software works.

ROM (Read-Only Memory): typically the area of a chip that holds the operating system and possibly parts of the application.

RSA (Rivest, Shamir, Adleman): a commonly used asymmetric cryptographic algorithm.

SAM (Security Application Module): a tamper-resistant computer component typically integrated into a terminal.

Scattering: the process of mixing the IC chip components so that they cannot be analysed easily.

Secret key cryptography: see symmetric cryptography.

Sequence number: a number attributed sequentially to a message and attached to it to prevent the duplication or loss of messages.

Server: a computer that provides services through a network to other computers.

Session key: a cryptographic key which is used for a limited time, such as a single communication session or transaction, then discarded.

Smart card: an integrated circuit card with a microprocessor, capable of performing calculations.

Stored-value card: a prepaid card in which the record of funds can be increased as well as decreased. Also called an electronic purse.

Symmetric cryptography: a set of cryptographic techniques in which devices share the same secret key in combination with algorithms. For encryption, the same key is used for encrypting and decrypting and the decrypting algorithm is the reverse function of the encrypting algorithm.

Tamper-evident: the capacity of devices to show evidence of physical attack.

Tamper-proof: the proven capacity of devices to resist all attacks.

Tamper-resistant: the capacity of devices to resist physical attack up to a certain point.

Time-stamp: a value inserted in a message to indicate the time at which the message was created.

TCP/IP (Transmission Control Protocol/Internet Protocol): a set of commonly used communications and addressing protocols; TCP/IP is the de facto set of communications standards of the Internet.

Transaction log: a sequential record of transactions that is stored on a device.

Transferability: in electronic money systems, the degree to which an electronic balance can be transferred between devices without interaction with a central authority.

Traceability: in electronic money systems, the degree to which value-transfer transactions can be traced to the originator(s) or the recipient(s) of the transfer.

White list: in a card-based system, a database containing the list of all authorised card numbers.

ANNEX 2

Models of electronic money systems

A. General model

In this model of various types of electronic money systems or products, three separate domains are defined (see Figure 1):

- the *clearing and settlement domain*, in which financial institutions, clearing houses and the central bank fulfil the interbank financial obligations resulting from electronic value transactions;
- the *issuing/acquiring/operating domain*, in which a structure is set up for issuing and acquiring electronic value as well as for interacting with the clearing and settlement domain; and
- the *retail domain*,[20] in which the actual value transfers between users take place:
  - loads: transfers of value from the issuer to users;
  - payments: transfers of value between users;
  - deposits: transfers of value from users to an issuer or an acquirer.

This annex focuses on the last two domains. It is assumed that readers are familiar with the processes that take place in the clearing and settlement domain, which are not specific to electronic money. For reasons of simplification, some flows such as the financial transfers between the various participants in the issuing/acquiring/operating domain resulting from the issuing and acquiring of electronic value are not represented here.

B. Sample models

Given that the arrangements in the issuing/acquiring/operating and retail domains can vary considerably, it is not possible to give an exhaustive overview of all possible models.

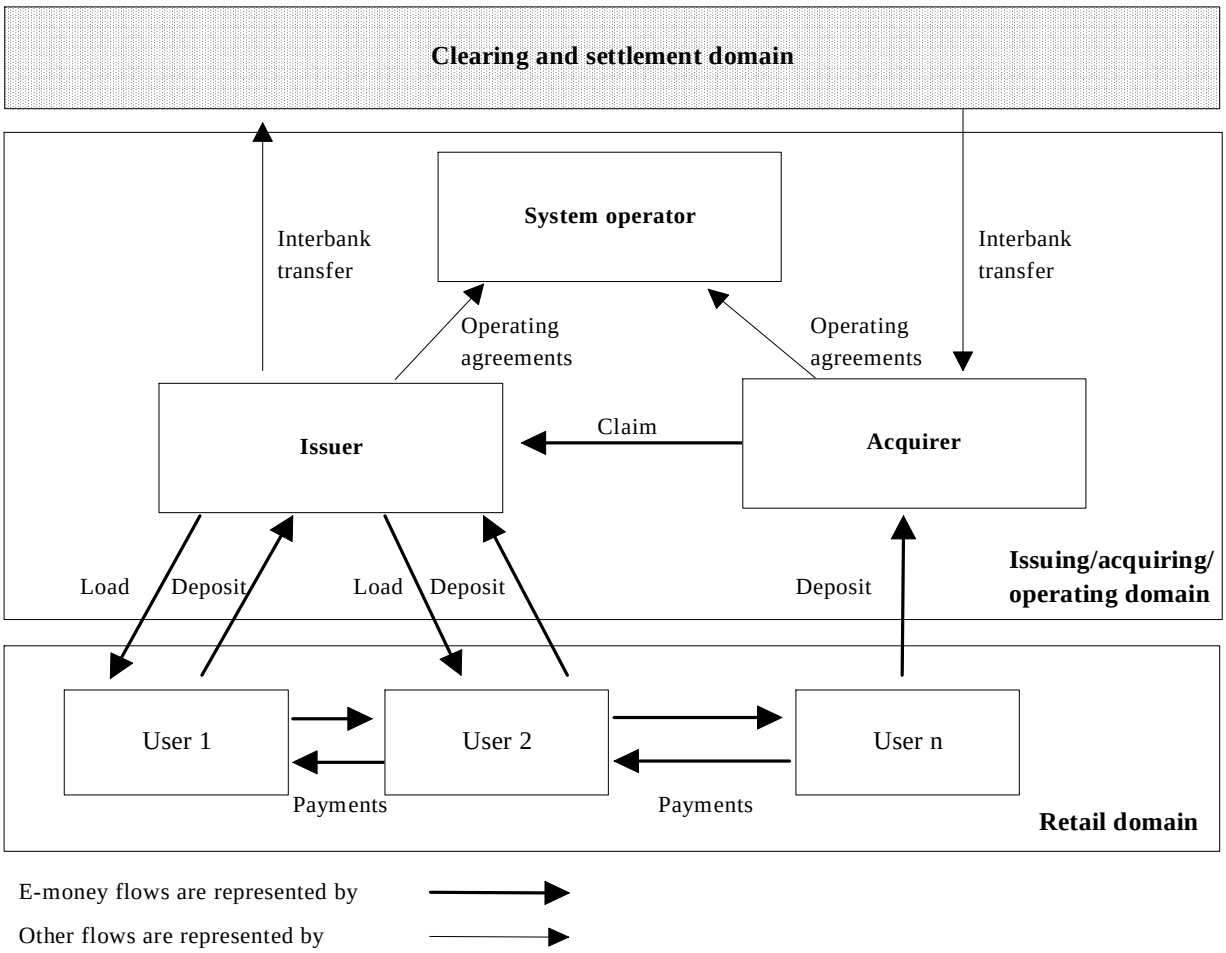
However, two simplified models of electronic money systems are presented here to illustrate the arrangements that take place among the entities in the issuing/acquiring/operating domain as well as the degree of transferability of value in the retail domain.

---

[20] In this general model, no functional distinction is made between the users of electronic value (consumers and merchants); electronic value can be freely transferred among these users. This situation is for the moment theoretical; as stated in the report, the Task Force did not encounter such systems providing unlimited transferability of electronic value in its investigations.

Figure 1

General model



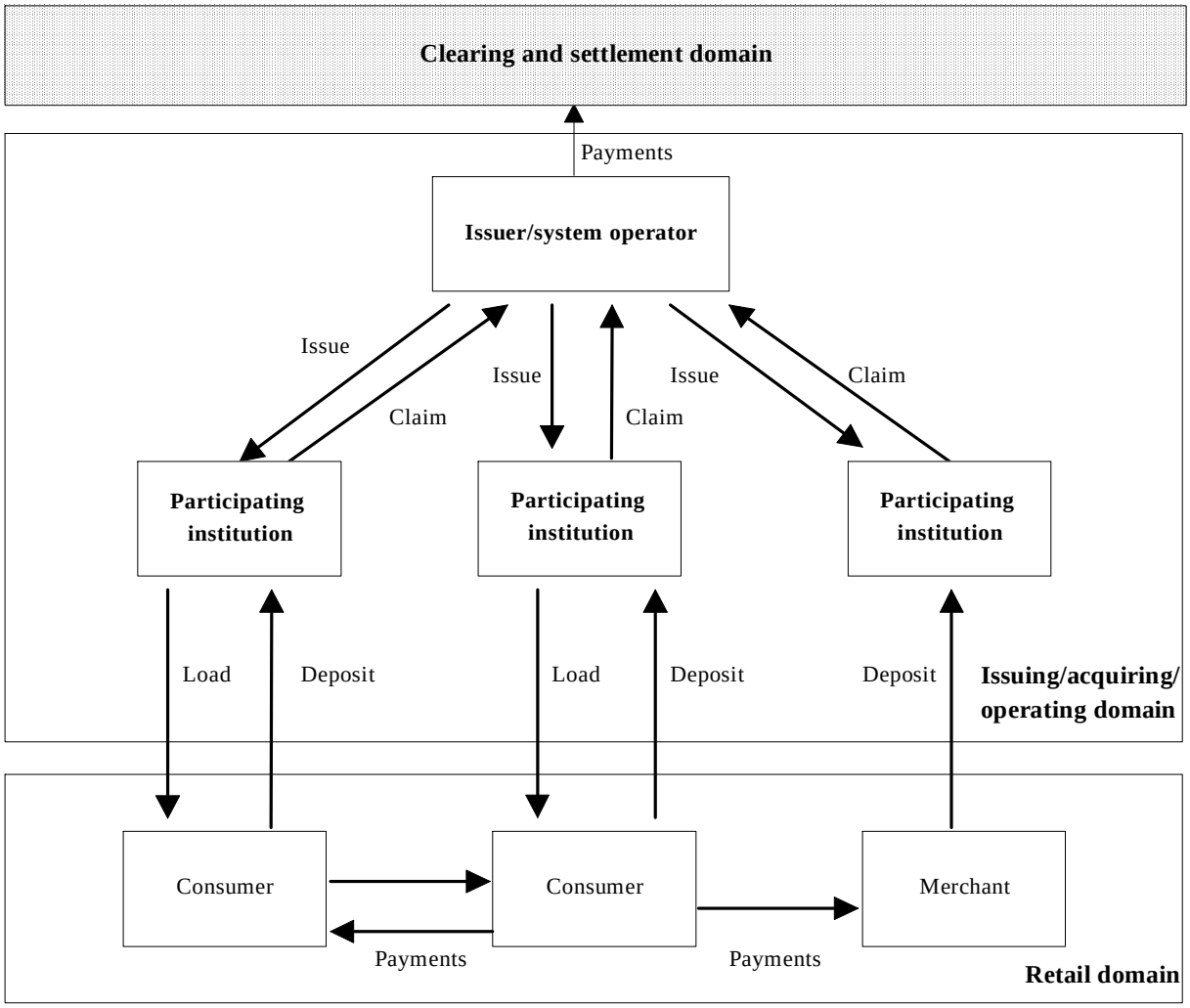
In the case of a single-issuer system (see Figure 2), the flows of value are similar to those that take place in cash payment systems involving an issuing institution (central bank), the banking system and the retail system. A single issuer creates electronic value and issues it to participating institutions, typically banks. These institutions load electronic value onto their clients' (consumers') devices; this electronic value is used by consumers for payments; merchants and consumers deposit these funds with their banks (participating institutions); the value is claimed from the issuer. The interbank payments resulting from transfers of electronic value (issuing and redeeming) are processed and effected in the clearing and settlement domain.

In such a model, the issuer will also typically be the system operator and the participating institutions will also play the role of acquiring institutions.

In the retail domain, consumers are allowed to transfer value freely between themselves (purse-to-purse transactions) and to merchants, but merchants are obliged to deposit the electronic value received as payments.

Figure 2

Single-issuer system with free transferability between consumers



In a multiple-issuer system (see Figure 3), the main entities in the issuing/acquiring/operating domain are the issuers, acquirers and system operator. Although in this model issuers and acquirers are distinct for reasons of clarity, it will often be the case that institutions are both issuer and acquirer.

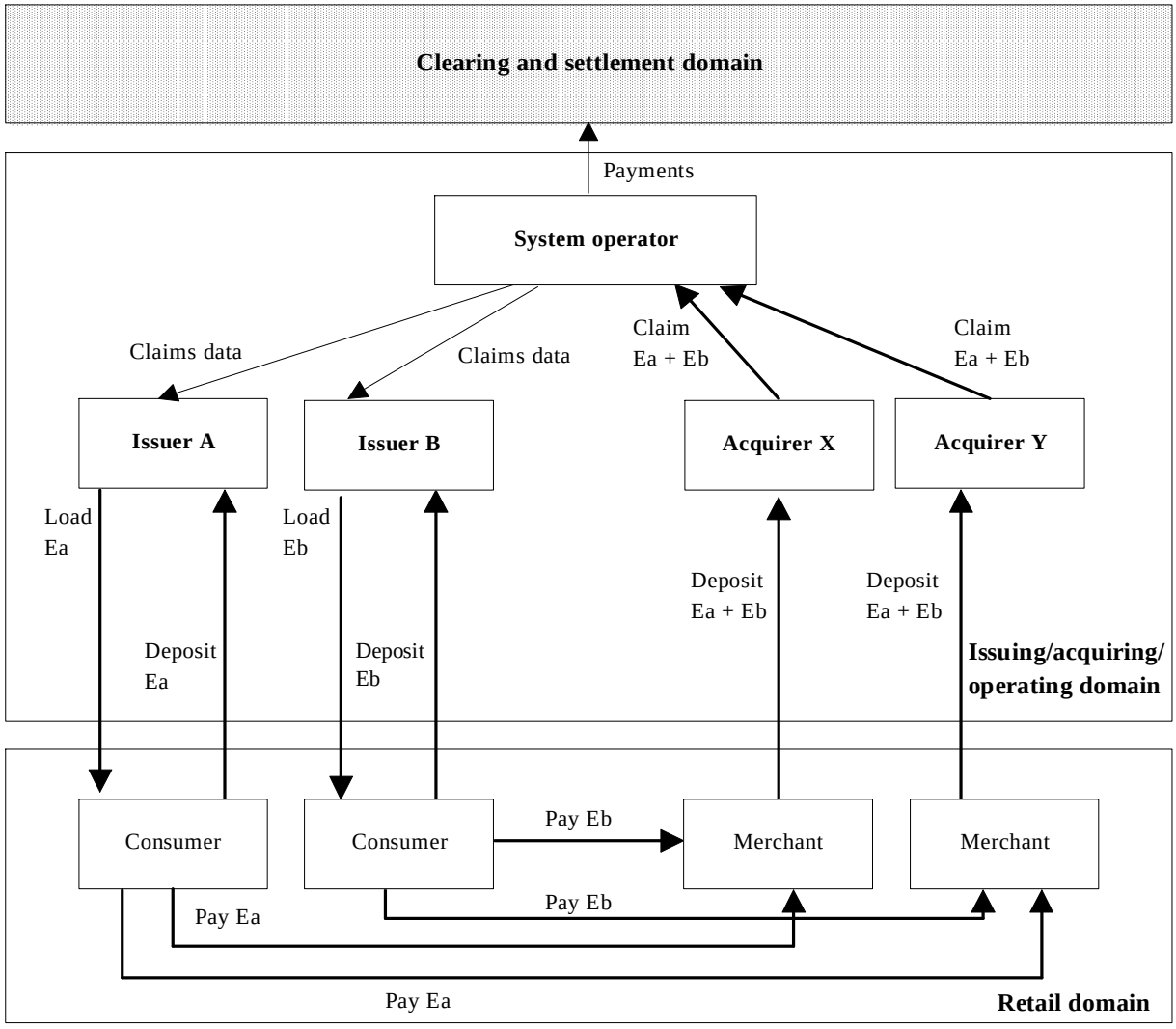
Each issuer creates and issues electronic money to its clients (consumers); merchants receive payments from consumers; merchants deposit these funds with their acquirer; the system operator collects from the acquirers the claims on the issuers, consolidates those claims by issuer and transmits the relevant information to them; the interbank payments resulting from these claims are processed and effected in the clearing and settlement domain.

In the retail domain, electronic value held by consumers can only be used for payment in transactions with a merchant; electronic value collected by merchants can only be deposited with acquirers. Consumers can deposit electronic value with their issuer.

Figure 3 provides an illustration of the possible functions carried out by a single system operator. However, system operators' responsibilities vary considerably and electronic money systems might have several system operators.

Figure 3

Multiple-issuer system with transferability limited to one payment transaction



Ea: electronic money issued by A

Eb: electronic money issued by B

ANNEX 3

Table of security measures

The following table provides an overview of the security measures commonly applied in card and software-based electronic money systems. The first part of the table sets out the security measures that are available to prevent, detect and contain the general fraud risks in such systems. It also describes some organisational measures that would provide protection against those risks. The second part of the table presents the security and organisational measures that are available to counter certain specific risks.

The distinction made between these measures (prevention, detection, containment and organisational) is sometimes arbitrary. It is obvious that some measures might be considered under more than one category. For example, measures that lead to the detection of fraud constitute a deterrent for potential criminals and might, therefore, also be considered as prevention measures.

It should also be underlined that this table is not to be seen as a list of mandatory security measures but rather as an inventory of security measures which the Task Force encountered in its investigation of electronic money systems. That is, not all systems utilise all measures.

	Prevention	**Detection**	**Containment**	**Organisational**
General measures				
	Devices containing secret or sensitive information provide protection (tamper-resistance) against analysis and non-authorised changes. Cryptography is used to authenticate transactions and devices and to protect data confidentiality and integrity. Load transactions and sometimes payment transactions are authorised online by the issuer.	Transaction details are collected, enabling the verification of financial and security data. Certain factors require the devices to interact with the central system so that security parameters or transaction logs can be checked and certain parameters updated. Limits are placed on the transferability of stored-value balances so that fraudulent balances can be detected more rapidly. Statistics on payment flows are collected and compared with certain predefined norms. Lists of suspicious cards are maintained by the issuers and kept by merchants.	Limits are set for the maximum balance(s) that a device can store. Limits are set for transaction amounts. Expiration dates are applied to devices, balances and security parameters. Sharing of secret cryptographic keys is avoided. Devices are linked to an account and device holders are registered. In the event of large-scale fraud the system is suspended.	Strict manufacturing and software development procedures are implemented. Security evaluation of components and procedures is carried out by third parties. Responsibilities of the participants are clearly defined. The initialisation, personalisation and distribution of devices are strictly controlled. The system is audited regularly.

	Prevention	Detection	Containment	Organisational
Measures against specific threats				
Duplication of devices				
	The manufacture of fraudulent devices and in particular of IC chips requires theft of hardware and software design, which are very well protected, and necessitates very substantial capital investment. Essential parts of the IC chip are physically protected against optical or electrical reading, and therefore cannot simply be copied or reverse-engineered. The secret data on the card needed to duplicate it are logically protected via encryption, scrambling or scattering.	All devices are registered. All devices contain a unique identification number certified by the issuer as well as unique cryptographic keys. Devices are authenticated during transactions. Devices are monitored by the central operator when they interact with it.	Merchant terminals hold lists containing the numbers or range of numbers of suspicious cards. Devices can be blocked or disabled by the central system.	The manufacturing, initialisation and personalisation processes are strictly controlled and carried out by different organisations. Inside these organisations, there is separation of staff responsibilities. Security evaluation of devices is carried out by third parties.
Alteration or duplication of data or software				
Generic measures	Data and software are stored in tamper-resistant devices.	Devices contain indicators of tampering attempts (tamper evidence) that are monitored when the device interacts with the central operator. Detection of suspicious parameters by a merchant terminal might force the purchase transaction to be authorised online.	Devices can be blocked or disabled by the central operator. Devices have expiration dates. The loading and collection processes are used by the central operator for updating the security parameter in the devices.	
Duplication of electronic notes		Notes are verified online.		
Creation of electronic notes	Notes are cryptographically certified by the issuer.	Notes are verified online.		

	Prevention	Detection	Containment	Organisational
Creation of transactions	Payment transactions are digitally signed using the key unique to the card. Transactions are authorised online. Devices are mutually authenticated.	Transaction sequence numbers are verified. Shadow-balance accounts are maintained. Unusual payment patterns are detected.		
Alteration of application, operating system software and static data (maximum amount, etc.)	Applications and operating system software are stored in physically protected memory areas (ROM) and are logically protected through scrambling or encryption.	Software checksums show evidence of alteration.		
Alteration of electronic value balance	Balance can only be modified upon the instruction of an authorised device.	Shadow-balance accounts are maintained.		
Alteration of messages				
Modification of messages	Challenge-response mechanisms are used to initiate the transaction. The message exchange is controlled by the transaction protocol and by the use of derived session keys. Message integrity is verified by a hash algorithm or a Message Authentication Code (MAC). Messages are authenticated by MAC or electronic signatures.	Electronic signatures are verified. Transaction sequence numbers are verified. Transaction time-stamps are verified.		

	Prevention	Detection	Containment	Organisational
Replay or duplication of transactions	Unique session keys are used. A PIN is required for load and deposit transactions by consumers.	Transaction sequence numbers are verified. Transaction time-stamps are verified. Shadow-balance accounts are maintained. Unusual payment patterns are detected.		
Theft or repudiation				
Theft of devices	Load transactions require the input of a PIN. Cards are actively polled by the issuer or the central operator.		Cards can be locked by their holders with a PIN. Cards can be blocked or disabled by the issuer. Limits are set on transactions or card amounts.	
Theft of electronic notes	See duplication of electronic notes.			
Repudiation	Transactions are logged by the issuer. A certain number of transactions are logged on the card and can be checked by the cardholder. Transactions are identified by sequence numbers and are time-stamped. Transactions are cryptographically signed by clients and merchants. A certification authority (CA) maintains a database of certified public cryptographic keys.			

	Prevention	Detection	Containment	Organisational
Malfunctions				
Transactions in an unbalanced state	Transaction protocols ensure that transactions are either carried out successfully or cancelled.	Errors during the transaction will be logged by both devices and corrected afterwards.	After a certain number of errors the device will be blocked and forced to interact with the central operator.	
Cryptographic attack				
Theft of cryptographic keys	Devices containing cryptographic keys are tamper-resistant. Secret keys are generated in a highly secure environment. Secret keys transported over networks are encrypted. Asymmetric cryptosystems, which do not require secret keys to be transported over networks or to be shared by devices, are used.	Terminals hold a list of (ranges of) compromised keys.	Secret keys and algorithms are changed regularly or can be changed in an emergency. Keys have an expiration date. In symmetric cryptosystems: - devices use different symmetric keys for specific purposes; - keys are derived; - master keys are partitioned among multiple devices; - session keys are used.	Strict key management is implemented. Cryptosystems are subject to third-party evaluation. Procedures are submitted to external audit. Published algorithms are used.
Breaking of cryptographic keys	Keys of a sufficient length are used.			

	Prevention	Detection	Containment	Organisational
Use for criminal activities, in particular money laundering				
		The transactions are uniquely identified. The transactions are signed electronically. The transactions (load or payment) are verified and authorised online. The devices are forced to interact with the banking system. Specific payment patterns are investigated.	Limits are set for the transferability of value. Limits are set for the maximum amount per device and per transaction. The devices holding value are registered and possibly linked to an account. The device holders are known.	Consumers and merchants are checked for criminal records. Financial institutions participating in electronic money systems are monitored.

ANNEX 4

The Internet

INTRODUCTION

The purpose of this annex is to provide an understanding of the Internet and an overview of Internet payment schemes in existence and under development. The Internet is constantly evolving, however, and any description will soon become outdated.[21]

OPERATION OF THE NETWORK

The Internet is a data infrastructure that connects computers via telecommunication networks. It originated in the 1960s and 1970s, when the United States Department of Defense Advanced Research Projects Agency (ARPA) funded a small group of computer programmers and electronic engineers to redesign the way computers were operated. This resulted in the creation of ARPANET, the first network of computers. Internet, the successor to ARPANET, was sponsored in the 1980s by the National Science Foundation and included tens of thousands of researchers and scholars in private industry and universities, connected to the network through their institutions' computer centres. It is estimated that by July 1995 the Internet consisted of 120,000 host computers, connecting 40,000,000 users through 70,000 networks.

Protocols and addresses

TCP (Transmission Control Protocol) and *IP* (Internet Protocol) can be considered the building blocks of the Internet. TCP and IP are communication protocols that control communication between all connected computers. The protocols are designed to establish links between all types of computer and network. The information elements (called "packets") sent over the network usually contain the addresses of the receiver and the sender. A large set of data can be split into several packets, which might follow different communication routes over the Internet and be reconstituted by the receiving machine.

Computers on the Internet each have a unique address. The physical addresses are linked to logical names in a "name server", analogous to a telephone book. Addresses are issued by the Internet Assigned Numbers Authority (*IANA*) under contract to the National Science Foundation. Currently the Information Sciences Institute of the University of Southern California is the executing office of IANA. Administrative tasks such as the issuing of addresses are delegated to Delegated Registries for certain domains or geographical areas.

The composition of the names used on the Internet illustrates the types of domain. The last part of the name is called the Top Level Domain Name (*TLD*). The TLD consists of two characters representing a country (using country codes conforming to ISO standard 3166) or three characters representing a certain domain ("com" for commercial, "gov" for the US Government, "edu" for educational institutions, "net" for Internet providers, etc.).

---

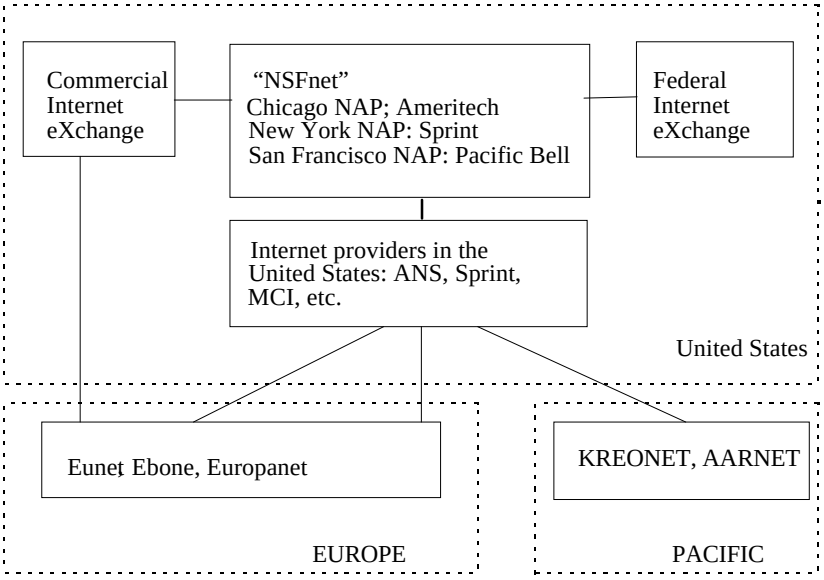
[21] The main source on which this annex is based is Jurg, P., and Zegwaart, E., Het Internet als digitale snelweg, Amsterdam, 1995.

Network structure

The network structure of the Internet is depicted in Figure 1. As the network structure is constantly changing, this diagram serves only to illustrate the fact that the Internet has a certain known structure. This structure is subject of discussion in several user groups that are concerned with standardisation and the architecture of the Internet. These groups include the Internet Architecture Board (*IAB*), which consists of experts who monitor the multiprotocol architecture of the Internet; the Internet Engineering Task Force (*IETF*), consisting of more than 600 individuals who contribute to the standardisation of security, applications, routing, network integration, etc.; the Internet Engineering Steering Group (*IESG*), which consists of representatives of the IETF and has the task of coordinating all IETF standardisation efforts; and the Internet Engineering and Planning Group (*IEPG*), consisting primarily of the operational network managers of Internet providers. The IEPG is concerned with providing a responsible and sensible design as well as the technical links between the Internet computers. The Internet Society (*ISOC*) is a more formal organisation which was established in 1992 to create an international forum for government, industry and individuals to discuss the rules and procedures governing the use of the Internet.

Figure 1

Network structure of Internet (Jurg and Zegwaart, 1995)



The future technical development of the Internet may depend on the continued provision of the information storage and transmission capacities needed for the increasing numbers of users. The IP address structure and the available bandwidth for communication are issues of concern.

APPLICATIONS AND USERS

In the 1980s, the Internet included tens of thousands of users who exchanged information using electronic mail ("e-mail"), "gopher" (menu-organised databases) and the file transfer protocol (ftp). Since 1990, the number of users and applications on the Internet has grown more rapidly as a result of recent developments, such as a progression from text-only information to multimedia information (including graphics, video and sound) and the availability of easy-to-use "browser" applications. Other factors have included the further stimulation and sponsoring of the Internet by governments (in particular the US Government), the declining prices of the necessary hardware and

certain telecommunications services, and the growing exploitation of the Internet by commercial enterprises.

The most well-known applications on the Internet include: *electronic mail* for the sending of electronic messages and documents between users; the *World Wide Web (WWW)*, including multimedia information, as discussed below; the *file transfer protocol (ftp)*, used to upload or download files to or from certain computers; *newsgroups* or discussion groups on specific topics; *gopher*, an application used to browse textual information; and *terminal emulation*, used to allow a computer to act as one of the terminals of a host mainframe or a host server. Other applications (e.g. telephone calls) do exist, but are not as widely used. Current research on the use of the Internet in the United States shows that the three applications used most often are e-mail (87%), the World Wide Web (79%), and file transfer (42%).[22]

THE WORLD WIDE WEB

The World Wide Web consists of information stored in a special format known as HyperText Markup Language (HTML). HTML information can be read by means of special applications, called *browsers*. Currently, browsers such as Netscape, Webexplorer, Mosaic and Spry are commonly used. Updates and improved versions of these browsers are regularly distributed via the Internet.

Information provided by a user or an organisation on the Internet is called a *home page*. The location of a home page is indicated by its address. For example, the address http://www.report.com indicates the use of the hypertext transfer protocol (*http*) and the location of the HTML file. A browser that is instructed to go to such an address will use the information in the HTML file at that location to display graphics, sound and text on the computer of the user.

An important feature of HTML is that it allows references to other Internet addresses to be included as part of the HTML code. As a result, it is possible to create links or pointers to other computers. The use of these links provides the user with a transparent view of information. Users do not have to know where the information is stored and can access information from all over the world, typically within seconds.

The fact that HTML applications allow many different users to communicate and interact leads many to expect that the Internet, and the World Wide Web in particular, will provide new shopping and business opportunities for consumers and merchants. To date, the following retailer approaches on the World Wide Web can be distinguished: use solely for information and advertising purposes; provision of both advertising and ordering facilities, with the subsequent payment being made via traditional channels (telephone, mail); and provision of payment facilities as well as advertising and ordering mechanisms. The 1996 Online Advertising Report indicates that the income of service providers on the Internet in 1995 was US$ 55 million, including US$ 43 million derived from providing advertising space on the World Wide Web, and US$ 12 million from providing online services to users.[23]

In general, it can be observed that Internet sites are developing rapidly. Experimental World Wide Web sites are designed to establish the most successful formula for doing business and making payments over the Internet. The low level of business income via the Internet is often explained by the lack of secure and cheap payment facilities on the Internet. A considerable amount of effort is, therefore, being invested in the development of such payment and ordering protocols.

---

22 Onderzoek Internet gebruik USA, Emnet No. 3, Alphen a/d Rijn, 10th February 1996.

23 1996 Online Advertising Report, Jupiter Communications; http://www.jup.com/

INTERNET PAYMENT SCHEMES AND THEIR PROVIDERS

As a result of the large number of initiatives to develop payment mechanisms for the Internet, it would be impossible to describe the Internet payment schemes and their providers in detail.[24] In general, the following types of payment scheme are available or under development:

- credit card orders transmitted by electronic mail without encryption;
- the use of encryption software for credit card orders;
- an electronic "cheque" system, software that permits users to create what are intended to be electronic equivalents of paper cheques that can be transmitted to retailers over the Internet and result in funds being transferred through the traditional clearing infrastructure from an existing bank account;
- electronic "notes", which are issued in exchange for prepayment by customers and are often promoted as a means of making very small-value payments; and
- home-banking services, in which the Internet is used as the transport network for payment orders and for the retrieval of sensitive customer information.

There are a number of different types of payment scheme provider on the Internet. Some banks and other financial institutions offer home-banking or payment facilities to their customers. In addition to home banking, banks can also offer more innovative payment systems such as those using electronic "notes", although such developments are not widespread to date. Some groups of retailers offer Internet shopping "malls" and payment facilities to their members. Consumers who register as a user or a member are able to pay for the products offered by the merchant members. Other payment system operators offer diverse schemes. Services range from encryption of credit card numbers to provision of an Internet interface for home-banking software. Third-party processing agencies provide facilities for payments using existing credit cards or bank accounts.

A number of universities and research laboratories have developed their own Internet payment schemes. Some of these have been developed for research purposes only; others are being tested in small pilot schemes. Often a major sponsor from the banking, payment or retail industry will be involved in such pilot schemes. Several industry consortia, including financial and non-financial organisations, are developing payment schemes for the Internet. Some aim to carry out pilot programmes of their systems in 1996.

INTERNET SECURITY

Security of protocols and servers

The TCP/IP protocol, which is the core component of the Internet, has been designed to provide a high level of resiliency with a minimum level of overhead network information in the messages. As a result the TCP/IP protocol does not provide for a high level of security. The following measures have been aimed at providing additional security: (1) the development of an additional protocol (Netscape Secure Socket Layer) to establish encryption between Internet client and Internet server; (2) the development of an extension of the http language (**s-http**, secure http), which

---

[24] Wayner, P., Digital Cash, Commerce on the Net, London, 1996. For other references to payment methods for the Internet, see for example:

http://ganges.cs.tcd.ie/mepeirce/project.html
http://www.wiso.gwdg.de/ifbg/banking.html

establishes a protocol by which an Internet client and an Internet server can negotiate the appropriate level of security before exchanging information; (3) an initiative by the IETF to extend the TCP/IP protocol to allow certain security functions.

Normally, servers on the Internet, also called "hosts", use a Unix operating system. As a result of the security design of Unix (in which a superuser has considerable control to perform specific read and write operations) and the fact that it is impossible to control all the existing superusers of the Internet servers, it must be assumed that communications on the Internet can be overheard, deleted and possibly altered.

Disclosure of information

It is fairly easy for certain experienced computer users ("hackers") connected to the network to intercept and read the flow of information involving other computers. Sophisticated software can be built to reside in the background of the application or operating system without the knowledge of the user. This software can be designed to intercept sensitive information such as passwords, PINs or credit card numbers, and send it automatically to a predetermined location on the Internet. Therefore, software transmitted over the Internet must be certified or checked to ensure that no unauthorised programs (known as "viruses") are present.

Unauthorised access

One of the major threats arising from the security limitations of the Unix-based operating systems on the Internet is unauthorised access to internal systems. Attempts at gaining such unauthorised access can be carried out by using stolen passwords, by impersonating a trusted user ("spoofing"), or by launching an attack from a host that is trusted by others. Software is readily available to analyse a specific network and to locate any security breaches. This software can, of course, also be used by hackers who may wish to attack a network. As a protection measure, all the communication between a computer (or an internal network of computers) and the Internet should be predefined and controlled. Such security measures are called *firewalls*.

Unavailability, unreliability and denial of service

There is no guarantee of service availability and continuity on the Internet. It cannot be assumed that messages will arrive at their destination without delay or corruption. It must be assumed that it is possible to overload a server with traffic in order to create a denial-of-service situation.

Security evaluation

Both protocols (TCP/IP) and components (mainly Unix-based servers) of the Internet have security limitations that make the Internet, by itself, an unsafe environment. It is therefore the responsibility of its users and product suppliers to ensure secure transfer of information or payment transactions over the Internet. Public key cryptography and digital signatures are the key technologies which provide for privacy and authentication.[25] In fact, the use of these technologies (provided that keys are stored in a tamper-resistant manner) can be viewed tantamount to creating private networks over the public network.

---

[25] **PGP** (Pretty Good Privacy) is an example of a software application that is used to provide such extra security.

ANNEX 5

Smart card security

INTRODUCTION

Currently, most payment cards still use a magnetic stripe to store consumer-related information. In the future, however, it is expected that extensive use will be made of integrated circuit (IC) cards for consumer payment systems, such as debit cards, credit cards and electronic purse systems. This annex provides a description of IC cards, the production and personalisation process and their security features.

IC cards can be categorised as smart cards or memory cards. A smart card has data-processing and storage functionality, whereas a memory card is used only for data-storage purposes. The first operational IC card systems for consumers (telephone cards in France) made use of memory cards. Currently, most systems use smart cards because of the data-processing functionality needed for computing, particularly cryptographic, purposes. Smart cards can be either of the contact type, which must be inserted into a reader when used, or of the contactless type, which must contain its own power source and operates remotely from the reader/writer. This annex focuses on the contact smart card, the device used in many electronic purse or stored-value card projects.

SMART CARDS

A typical smart card is a plastic card in which an IC chip is embedded and on which eight contacts are placed. The physical and electronic specifications generally follow ISO and IEC standards (see Annex 6). A typical smart card chip consists of the following components:

CPU (Central Processing Unit), which performs computation;

ROM (Read-Only Memory), which stores the operating system and applications;

EEPROM (Electronically Erasable and Programmable ROM), which stores the variable data such as the balance of the purse, cardholder data, etc.;

RAM (Random Access Memory), which is used as the work area when the chip is processing; and

I/O (Input/Output), which takes place through designated contact fields.

The price of a smart card depends on its data-storage and processing functionality. Smart cards with limited memory (8 Kbytes) and built-in symmetric encryption processors are currently available at a relatively low price (approximately US$ 5 if produced in large quantities). Smart cards that can also perform asymmetric cryptography have, in the past, been considered much more expensive and technically less reliable. In the course of 1996, a new generation of more reliable IC chips that contain a coprocessor to compute asymmetric cryptography are expected to become available at reasonable prices.

THE PRE-OPERATIONAL STAGES OF THE IC CARD LIFE CYCLE

The development and the production of IC cards is a very complex process, consisting of roughly the following phases: design, manufacturing and initialisation of the chip module; embedding of the chip module in the card; and personalisation. Many controls and measures are implemented to

ensure that no single entity or person can obtain complete knowledge of the design of the chip, the cryptographic initialisation keys, or the initialisation or personalisation data. Separation of duties on a need-to-know basis is common during these early phases of the IC chip life cycle. This can be achieved through cryptographic separation, physical separation, in which two or three employees are needed to produce or transport certain keys, or administrative measures, including internal controls.

Design and manufacture of the IC chip

The chips that are being used in smart cards are produced mainly by a few large manufacturers. The technical characteristics of chips from these manufacturers determine the constraints within which electronic money suppliers and others must design the functionality of their IC chips. It should be noted that the manufacturers do not provide their technical design to potential customers; rather, they provide only the set of commands that the chip operating system can execute.

Organisations can choose between designing their own proprietary application code in close collaboration with the manufacturer and buying a standardised application that has already been designed by the manufacturer. The application code must be extensively tested before being converted into a "mask", which is the hardware specification that defines the physical and functional properties of the IC chip.

The production of chips takes places in several steps. Chips are first produced on a silicon wafer; then the wafer is sawn into smaller parts. The chips are mounted on separate modules, encapsulated with coatings and then tested, after which the test pins that are used during this phase are physically disabled.

As a final step in the production process, the chip module is initialised. The EEPROM is programmed to contain the directory and file structure. In addition, the most important cryptographic keys are loaded during this phase in order to provide control over the subsequent phases.

Embedding the chip module in the card

The process by which the chip module is mounted on the plastic carrier is called embedding. The company that performs the embedding function does not have access to the secret cryptographic keys with which the chip is protected, and therefore cannot tamper with the contents of the chip.

Personalisation

During the personalisation phase, the application on the chip is uniquely identified and the chip is loaded with all necessary personal and non-personal data and secret cryptographic keys. This process is divided into several steps and can also be designed to be performed by separate companies. The issuing company is present during all steps in this process, to control and supply the necessary keys.

The personalisation of the smart card takes place in such a way that the personalisation company cannot read the user data. The user data are encrypted by a key that has been loaded by the card-issuing organisation during the initialisation phase. This encrypted information is then decrypted by the card itself using the same secret key and stored in the appropriate records and files on the card.

SECURITY MEASURES

The countermeasures that can be taken to protect IC cards relate to different threats and vulnerabilities, such as analysing its design optically or electronically, manufacturing a fraudulent IC card, or changing the content of the IC chip (for example by increasing the balance).

Measures to prevent optical and physical analysis

Code in ROM is invisible. In the past, the ROM code was implanted on a chip with transistors that could be easily read optically. With advanced technology, the code is now usually implanted using the density of impurities in the transistors, and is protected by special coatings in order to prevent optical analysis.

Layout of chip is scattered. In earlier designs, the components of an IC chip such as the CPU, ROM, EEPROM, RAM and I/O were clearly separated on a chip, which made it easier to isolate each component from the others and analyse them separately. It is difficult to do so with an advanced IC chip, because the important components are scattered across different areas of the chip.

Double metal layer of wiring. Chip wiring laid out in a single layer may be relatively straightforward to analyse. With current advanced technology, however, the wiring is distributed between two layers, which makes analysis more difficult. The inclusion of "dummy" wiring in some chips is also intended to deliberately mislead potential attackers.

Measures to prevent electrical analysis

Low-frequency detector. Electrical analysis of IC chips is done by measuring the voltage and current of the wiring when the chip is working at very low frequency. With the current technology the chip is designed in such a way that it will not operate at low frequencies.

Scattered ROM/EEPROM data. The data stored in the ROM and EEPROM in a chip are stored in different physical locations on the chip, so that an attacker who reads the contents of ROM and EEPROM faces the task of determining which bits belong together.

Disabled test pins. The test pins of the chip, through which the chip is tested during the manufacturing process, are physically disabled so that they cannot be used to gain access to the inside of the chip. This is also referred to as "blowing the fuses".

Use of sensitive wiring. The wiring of a chip is designed to operate at a certain voltage. If an attacker used a voltage above the prescribed levels to analyse the contents of the chip, the wiring would burn and the information on the chip could not be recovered.

Measures to prevent the manufacture of fraudulent IC chips

Small-scale technology. The utilisation of small-scale chip technology requires an investment of hundreds of millions of dollars in specialised equipment and extremely specialised expertise in order to manufacture an IC chip.

Proprietary operating systems. All chip operating systems are proprietary. Chip manufacturers generally provide a limited set of commands that the operating system will accept. They do not provide the source code.

Custom-made masks. Chip manufacturers and card issuers work closely together to establish the source code that will perform the specific application on the chip. This code is integrated into the mask, which is used to physically produce the chips. The code is known only to the manufacturer and developers.

Layout and keys during initialisation. The further layout of the data and the master cryptographic keys are established and loaded during the initialisation phase and are known only to the card issuer or other owner of the application on the chip.

Encrypted personalisation. Personalisation takes place by encrypting the user data under a cryptographic personalisation key that is known only to the owner of the application. This key is installed in the chip during initialisation.

Administrative and procedural controls. Administrative and procedural controls help ensure that no one person will be able to obtain all the information needed to fraudulently create a card.

Measures to prevent alteration of the contents of an IC chip

Electrical protection of EEPROM. A special protection layer protects the contents of the EEPROM from UV (ultraviolet) rays, X-rays and electromagnetic modification.

Commands for changing the contents of EEPROM. Changing the contents of the EEPROM requires several consecutive commands. The contents of the EEPROM cannot be altered unless the attacker can provide all the necessary commands in the proper order.

Control registers. For some data records stored in the EEPROM, a "hash" value (see Annex 7) is calculated and stored on the card in a control register. Access to the data records may only be allowed if the recomputed hash value is the same as the value in the control register.

EVALUATION OF IC CARD SECURITY MEASURES

To date, there have been no published reports of security breaches of smart cards, although some instances of tampering with simpler memory cards are known. Tampering with a chip would entail overcoming many physical and cryptographic barriers. This does not mean that the current security measures will continue to be sufficient in the future. As new techniques for attacking chips are developed, the current security measures may become obsolete and new ones will have to be adopted. In addition to new physical security measures, systems utilising IC cards should be designed to allow the security of the IC card to be upgraded, for example by implementing new or redundant algorithms.

Although not discussed in detail here, it should be stressed that considerable care must be taken to implement administrative and procedural security measures effectively. In view of the robustness of the technical security features of smart cards, an attack on administrative security during the manufacturing, distribution or issuing process (such as stealing ready-to-distribute cards, etc.) may constitute a greater risk.

ANNEX 6

Standards

INTRODUCTION

Most of the card-based products studied by the Task Force make use of one or more international technical standards in their design and implementation. These standards have been developed by formal international standardisation bodies, such as ISO and CEN, and by payment industry groupings such as EMV. This annex describes the main technical standards mentioned by the electronic money schemes examined and provides some information on the bodies which created them. (Other international and national standardisation bodies or industry groupings not mentioned may also be developing relevant standards.)

By contrast, there appear to be no international technical standards specifically related to software-based electronic money schemes. However, this annex notes some recently developed standards for electronic payments over open networks such as the Internet (and the processes used to create general Internet standards are described in Annex 4).

Both card-based and software-based products also make extensive use of cryptographic algorithms and techniques, as described in Annex 7. All the products examined intend to use publicly available algorithms, as published by national or international standards bodies or by academic or research organisations.

The use of international technical standards, whilst making electronic money products similar in certain respects, and even introducing an element of compatibility between them, does not ensure that they are, or will become, interoperable. It is possible that the interoperability of card-based products will only be achieved at the level of merchant and bank terminals, in that a single terminal will be able to process cards belonging to rival schemes. Whilst it is also possible that two or more electronic money products could reside on a single card as separate applications, the business case for this is not clear.

ISO

The members of the International Organization for Standardization (ISO) are national standardisation bodies (e.g. ANSI, DIN and BSI). ISO works through a formal structure of committees, subcommittees and working groups, and uses a formal procedure of drafting, review and voting to develop its standards. This structure does not always result in the timely production of standards, or production of sufficiently specific standards. However, ISO does have a "fast track" procedure, which allows standards that have been fully developed by other bodies to be adopted unamended as ISO standards. ISO has published a number of standards relevant to electronic money schemes, some of which have been developed jointly with the International Electrotechnical Commission (IEC).

All the card-based products reviewed by the Task Force used integrated circuit cards (IC cards) developed to the ISO standard "Identification cards - Integrated circuit(s) cards with contacts" (ISO 7816). This standard defines the design characteristics of generic IC cards (i.e. not specifically related to financial transactions), and was published in several parts between 1987 and 1995. The first part defines the physical characteristics of IC cards; the second part, the dimensions and location of contacts; the third part, the electronic signals and transmission protocols; the fourth part, the inter-industry commands for interchange; and the fifth part, the numbering system and registration procedure for application identifiers. (ISO 7816 was itself based upon earlier, more general ISO

standards for identification cards: "Identification cards - physical characteristics" (ISO 7810); "Identification cards - recording techniques" (ISO 7811); "Identification cards - numbering systems and registration procedure for issuer identifiers" (ISO 7812); and "Identification cards - financial transaction cards" (ISO 7813).)

The other ISO standards mentioned by one or more of the card-based schemes reviewed related to one of two categories:

- firstly, message exchange protocols, such as "Financial transaction card originated messages - interchange message specification" (ISO 8583) and "Financial transaction cards - messages between the integrated circuit card and the card accepting device" (ISO 9992);
- secondly, security-related standards, such as: "Banking - PIN management and security" (ISO 9564); "IT security techniques - digital signatures" (ISO 9796); "Financial transaction cards - security architecture of financial transaction systems using integrated circuit cards" (ISO 10202); and "Banking - key management (retail)" (ISO 11568).

CEN

The members of the European Committee for Standardization (Comité Européen de Normalisation) - (CEN) are eighteen European national standardisation bodies. CEN's function is to produce standards specific to Europe and to transpose international standards, such as ISO standards, for European use. Its work is recognised, and partly funded, by the European Commission. Like ISO, CEN works through a formal structure of committees, subcommittees and working groups, and uses a formal procedure of drafting, review and voting to develop its standards.

As part of a European Commission programme to establish international standards for inter-sector identification cards and other applications based on IC cards, a CEN working group (TC224/WG10) was set up in January 1991 to develop a European standard for an Inter-sector Electronic Purse.

This standard, prEN 1546, which is in four parts and still in draft form, is intended to cover most models of card-based electronic money and a wide variety of options. It supports: payments in any sector; a multi-application concept; contact and contactless IC cards; symmetric and asymmetric cryptography; open (many issuers) or closed systems; IC cards with or without a related bank account; manned and unmanned payment situations; systems with or without cardholder identification; and full accounting or truncation of data from terminal to issuer. However, the standard assumes that payments would normally be made offline, but that loads would normally be online.

Compliance with prEN 1546, and in particular the funds transfer message exchange protocol, was indicated by many, but not all, the European card-based schemes examined by the Task Force.

EMV

In December 1993, Europay International, MasterCard International and Visa International formed a joint working group (known variously as EMV or VME) to develop a common set of technical specifications for the use of IC cards by the payments industry, based on the available ISO standards, in particular ISO 7816. The purpose of the specifications was to provide the payments industry with a foundation upon which card-based applications could be developed. They were intended to define the minimum functionality necessary to support international interoperability between IC cards, terminals and related devices. They also sought to establish a high minimum level

of security for IC cards and terminals, to deter counterfeiting and other types of fraud, although individual products could provide additional levels of security.

Between June and October 1994, EMV published the first draft of a three-part technical specification, "Integrated circuit card specifications for payment systems". The first part of the specification defined the physical and electrical characteristics of IC cards and terminals, as well as the hardware interface that allows cards and terminals to communicate with each other. The second part defined a common set of data elements and commands sent between the IC card and the terminal. The third part defined the flow of transactions between IC card and terminal, the procedures to be followed by the terminal in processing a transaction, and the process of selecting a card application. (This part only defined a set of common core functions that all conforming IC cards could perform in all conforming terminals. Functions unique to an application, and those not performed in interchange, were not defined; neither were clearing, settlement, or any transaction where the card was not present.)

In June 1995, EMV published an updated version of the IC card specification, together with a second specification, "Integrated circuit card terminal specification for payment systems". This document defined the technical specifications of all types of terminal, including automated teller machines, point-of-sale terminals and personal computers. It also defined terminal security and the messages between the terminal and its host system.

EMV published on 11th July 1996 updated versions of the IC card and terminal specifications, together with a new "Integrated circuit card application specification for payment systems". New material in these documents includes specifications for: public key security; secure messaging (ISO and proprietary options); dynamic data authentication and terminal software architecture (both the Application Program Interface and Open Terminal Architecture approaches). These documents do not include the expected specification for an international stored value card or electronic purse. EMV is also understood to be working on other aspects of IC card implementation, such as: card production security; card personalisation processes; product and vendor approval for cards, terminal and related items, common card production masks and operating systems; and patents.

Compliance with the EMV specifications was indicated as a goal by most, but not all, the card-based schemes examined by the Task Force. It is possible that the EMV specifications will be offered to ISO for adoption as an international standard, through the "fast track" process, if a national standardisation body could be found to sponsor them.

ETSI

A standard for the interoperability of the IC cards used in portable GSM telephones (standard T9) has been created under the auspices of the European Telecommunications Standards Institute (ETSI). Two European card-based electronic money schemes propose basing their products on the T9 standard, although adaptations and extensions will be necessary to provide adequate security.

INTERNET PAYMENT STANDARDS

In the second half of 1995 two separate draft specifications for making secure payments over insecure networks such as the Internet were published: the Secure Transaction Technology (STT) sponsored by Visa International and Microsoft, and the Secure Electronic Payment Protocol (SEPP) sponsored by MasterCard International. However, in early 1996 Visa International and MasterCard International published for comment a joint draft specification called Secure Electronic Transactions (SET). SET is aimed at transactions made using existing payment products, such as credit and debit

cards, rather than electronic money products. The specification identifies five parties to any transaction: the cardholder, issuer, merchant, acquirer and payment gateway. The cardholder initiates the purchase across the network from his personal computer. Use is made of "trusted software" and authentication information on the PC.

SET specifies the use of message encryption, digital signatures and cryptographic certificates to provide confidentiality of information, integrity of payment data and authentication of cardholders and merchants. SET specifies RSA-based cryptography using 768, 1,024 or 2,048 bit keys and a hierarchy of certification authorities.

ANNEX 7

Cryptography

INTRODUCTION

The use of cryptography is a very important security measure in the design of payment systems and message protocols. Cryptography (literally: secret writing) can be viewed as the application of mathematical theories to realise a certain level of security or secrecy. The application of cryptographic theories and functions can help achieve objectives such as confidentiality, data integrity and authentication. This annex describes the building blocks of cryptography as well as their application within payment systems. It is intended to provide an overview of the most important cryptographic algorithms and tools.

GENERAL PRINCIPLES AND BUILDING BLOCKS

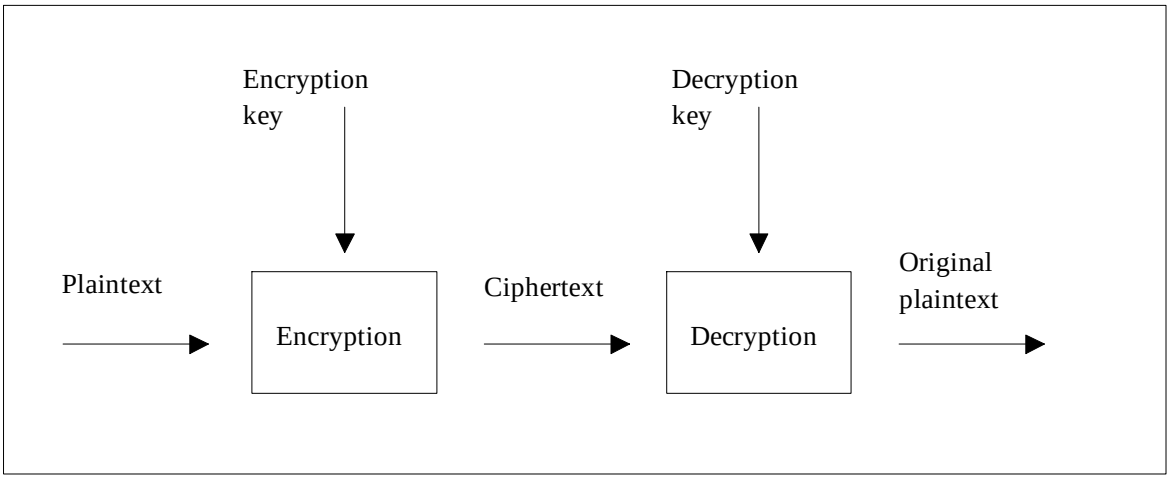
In this section, the general principles and terminology of cryptography are introduced and an overview of the most important cryptographic concepts is provided. These include encryption and decryption, one-way hash functions, challenge-response protocols with random numbers, digital signatures and key management.

Encryption and decryption

Confidentiality of data can be achieved by applying encryption or encipherment techniques. Senders and receivers of information can agree on a certain method of encryption and decryption to ensure that their message is not understandable to others. The encryption and decryption processes (see Figure 1) will require a mathematical function called an algorithm as well as keys, which are used to parameterise the encryption or decryption algorithm.

Figure 1

Encryption and decryption



Symmetric and asymmetric algorithms

An algorithm is called *symmetric* if it uses the same key as both the encryption key and the decryption key. The use of such an algorithm depends on the key being safely stored by the sending and receiving parties. Compromising the encryption key would allow outsiders to decrypt the message. The Data Encryption Standard (DES) is an example of a symmetric algorithm. DES was adopted by the US Federal Government in 1977 and was developed by IBM under contract to the National Bureau of Standards, now called National Institute of Standards and Technology (NIST).

Another class of algorithms, called *asymmetric* algorithms, does not use the same key for encryption and decryption, but makes use of a pair of different but mathematically related keys. One key is kept secret by the creator of the key pair (the private key) and the other key is made known to the correspondents of the key creator. A message encrypted with one key of the pair can only be decrypted by the other key of the pair. It is not possible to deduce one key from the other. Thus, a message encrypted by the sender with the receiver's public key can only be decrypted by the receiver using its private key. The Rivest-Shamir-Adleman (RSA) algorithm is an example of an asymmetric algorithm.

Asymmetric algorithms can also be used to provide authentication. If a message or part of a message is encrypted using the sender's private key and it can be decrypted using the sender's public key, the message can be authenticated, or assumed to have been sent by the sender. As asymmetric public keys can be held by many parties who may not know the holder of the private key, a *certification authority* is sometimes used to distribute public keys and to certify their relationship to the holder of the private key.

Generally, symmetric algorithms (such as DES) can be executed faster than asymmetric algorithms (such as RSA) because asymmetric algorithms require more processing time and resources. As a result, prices for computer hardware that can perform DES calculations are lower than those for hardware that can also execute the RSA algorithm. Consequently, those suppliers implementing encryption algorithms on IC chips concentrated first on implementing DES, but are now moving towards implementing RSA calculations.

Strength of encryption

The most desirable review of security algorithms consists of a public review by as many cryptographic experts as possible in order to analyse and detect any weaknesses in the design of the encryption method. If an encryption algorithm has withstood this review (cryptanalysis) for a considerable time, one can be reasonably sure that it does not contain secret "trapdoors" or undetected weaknesses. The use of public and extensively reviewed algorithms is therefore an important security principle, and one that is often applied by suppliers of electronic money systems.

The strength of the encryption should not be based on the secrecy of the applied algorithm, but on the fact that the secret and private encryption and decryption keys are known only to the sender or receiver of the message. It is therefore very important to store these keys safely and to use encryption and decryption keys of sufficient length.

To assess the strength of encryption algorithms, it can be assumed that the algorithm and the ciphertext are known to an outsider. An outsider could try to discover the plaintext by testing all possible decryption keys. This type of attack is known as a *brute-force attack* or an *exhaustive key search*. The amount of processing resources needed to discover the correct decryption key through a brute-force attack for a given algorithm and a given key length can be calculated relatively easily.

A group of cryptographic experts recently concluded that technology currently available makes brute-force attacks against symmetric cryptographic systems with small key lengths both fast

and cheap.[26] To provide adequate protection against the most serious threats, such as well-funded commercial enterprises or government intelligence agencies, key lengths of at least 90 bits are recommended for newly deployed systems. It is estimated that this key length will be adequate for the next 20 years. As far as asymmetric cryptographic systems are concerned, similar estimates are available, indicating that key lengths of 512 bits should be replaced by longer keys (768, 1,024 or 2,048 bits).

It should be noted, however, that key length itself is not a guarantee of a safe system. The complete spectrum of security measures (organisational, procedural and technical measures) will determine the security of a given system. The necessary key length will depend critically on the context in which the information must be secured. It is, therefore, not appropriate to presume that a system that applies the RSA algorithm with a key length of 768 bits is safer than a system for which a key length of 512 bits has been chosen.

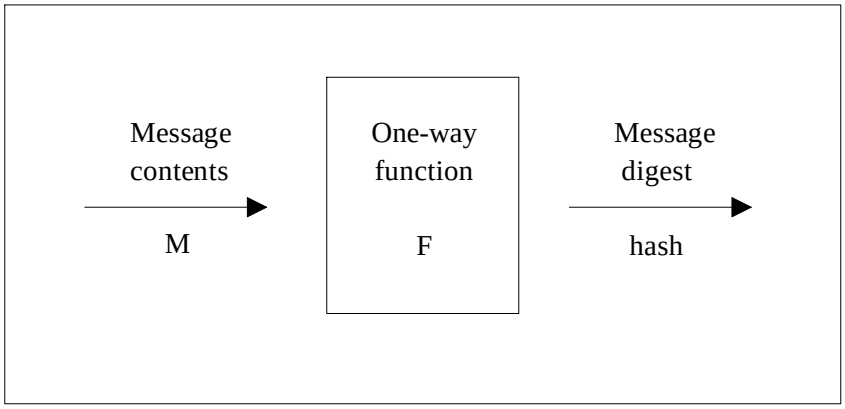
Furthermore, developments within cryptography are directed not only at new algorithms but also at cryptanalysis of algorithms, an area in which significant improvements can be expected in the years to come. In particular, progress with respect to so-called differential and linear cryptanalysis could force system designers to re-evaluate the key management schemes and to update the security of the systems.[27]

One-way hash functions

A one-way hash function is a means by which a receiver of a message can verify that the message content has not been changed. The sender of the message uses the message text and the one-way hash function to generate a hash value. The receiver of the message repeats this action and compares the received hash value and the calculated hash value. If they are the same, it can be assumed that the message content has not been changed.

Figure 2

One-way hash functions



[26] Blaze, M., Diffie, W., Rivest, R.L., Schneier, B., Shimomura, T., Thompson, E. and Wiener, M., Minimal key length for symmetric ciphers to provide adequate commercial security, Report by an ad hoc group of cryptographers and computer scientists, January 1996.

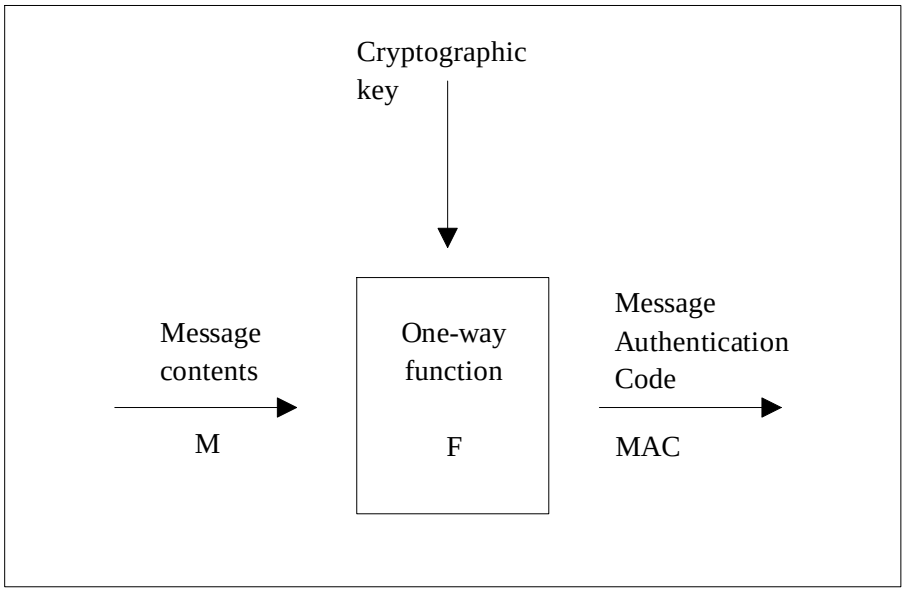
[27] Dr. Dobbs Journal, Differential and Linear Cryptoanalysis, January 1996.

An essential characteristic of a one-way hash function is that it can only be computed in a single direction and cannot be reversed. Furthermore, it may not generate the same hash value for different messages. In order to limit the risk of generating the same hash value for different messages, an appropriate hash function and an appropriate length of the hash value (for example 128 bits) must be selected. Hash functions are also subject to public review by cryptographers and are treated in the same manner as encryption algorithms. Well-known hash functions include Message Digest 5 (MD-5) and the Secure Hash Algorithm (SHA).

Through the combination of a hash function with the use of cryptographic keys, only parties that possess the appropriate cryptographic key can be permitted to verify the hash value. This is a more complex process, depicted in Figure 3. The result of the function is called a Message Authentication Code (MAC).

Figure 3

Computing a Message Authentication Code



Challenge-response protocols

Challenge-response protocols are used to establish whether two entities involved in communication are indeed genuine entities and can thus be allowed to continue communication with each other. One entity would challenge the other with a random number on which a predetermined calculation must be performed, often including a secret or a private key. In order to be able to generate the correct result for the computation, the other device must possess the correct private key and therefore can be assumed to be authentic.

The use of random or unpredictable numbers presents an attacker with an extra barrier, because past challenge and response values are not useful. The attacker will not be able to fraudulently authenticate a device by replaying an earlier recorded response because every response depends on a random input.

Digital signatures

A digital signature is a string of data, cryptographically generated, which authenticates both the sender and the contents of the message. Public key algorithms can be applied to provide digital signatures. Digital signatures in an asymmetric cryptosystem typically consist of encrypting a message or part of a message with a private key. Any recipient having the corresponding public key will be able to decrypt the ciphertext. Because the ciphertext can only be created using the private key known only to the sender, the recipient will have proof authenticating the sender of the message.

One use of digital signatures would consist in both parties performing the above procedure, thereby preventing denial, or repudiation, of messages after the event by either party. Depending on the system design, it might also be appropriate to include the time and date in the message. It is also possible for information to be time-stamped and digitally signed by a third party, thus attesting that the document existed at the stated time.

Digital signatures are not necessarily based on the mathematical problem of factoring. Signature schemes can also be based on other mathematical principles, such as the discrete logarithm problem.[28]

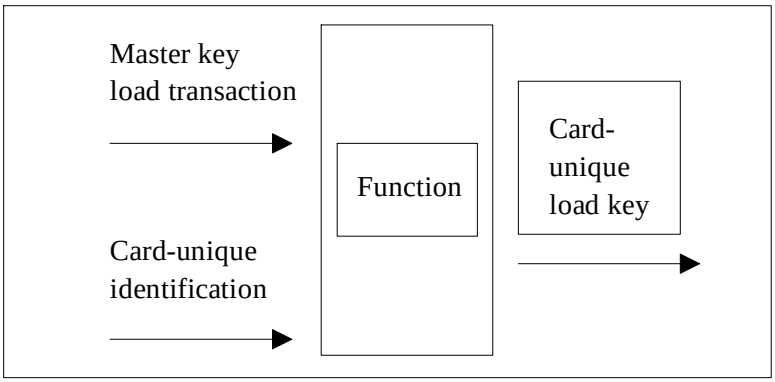
Key management

Payment systems employing symmetric cryptography that use a single system-wide cryptographic key for encryption, decryption and authentication purposes would be vulnerable to attackers, who would only have to discover the single key to manipulate any aspect of the system. Designers of payment systems, therefore, abide by certain key-management practices that have been established in international standards on key management, such as ISO standards 10202, 11166 and 11568.

As a principle of sound key management, cryptographic keys are only used for one specific function. A load transaction is secured by a special load key, a purchase transaction is secured by a purchase key, a collect transaction is secured by a collect key, etc. Furthermore, keys are unique to a card or terminal, so that the compromising of a card or terminal key would contain the security breach primarily to this individual level. These card-specific keys are created by a process called *key derivation*, which is depicted in Figure 8.4. This process typically takes place during personalisation of the card and can be applied to generate all the card-specific keys (card load key, card purchase key, etc.).

Figure 4

Key-derivation procedure



[28] Schneier, B., Applied Cryptography, New York, 1996.

In order to calculate a card-specific load key, for example, an arithmetic function is typically used that combines the system master key for load transactions with the card-specific identification number, for example the IC's serial number. The resulting value is used as the card-specific load key, which is stored in the IC chip. Whenever this particular card performs an online load transaction, the issuing bank reads the serial number of the IC card and recalculates the card's load key. In that way, both sides of the communication channel share the same individual key during the load transaction.

In addition to the use of derived keys, *session keys* are used as unique keys for every communication session. Session keys are special types of derived key that are based on the card's unique purchase keys, in combination with the transaction number of the card. The transaction number is derived from the card's transaction counter, which automatically increases for each transaction performed during the life of the card. A terminal holding the appropriate cryptographic key that receives the card's transaction number can recalculate the session key and use that key during a purchase transaction. The existence of these keys is limited to one session or transaction. New transactions will result in session keys with different values. The interception or possession of a session key will therefore not benefit an attacker for future use.

CRYPTOGRAPHY IN PAYMENT SYSTEMS

Applying cryptography to implement a secure payment system requires not only decisions with respect to the type of algorithms used but considerations regarding key management and key storage as well. Although these subjects are described separately, they are highly interdependent.

Use of algorithms and functions

The cryptographic principles and building blocks described above are used to achieve security goals such as confidentiality, data integrity and authentication. *Confidentiality* is typically achieved by using DES as the encryption method. Although it can also be done by applying asymmetric algorithms, owing to performance and price considerations the symmetric algorithms are generally preferred.

DES is also referred to as single-DES, to distinguish it from triple-DES. Triple-DES encryption consists of three consecutive operations (encryption; decryption; encryption) in which two DES keys are used (or a double-length DES key). Triple-DES has been developed in response to the increasing processing capabilities of computers and ensures that an exhaustive key search would still demand a considerable amount of resources.

Several governments have established strict rules with respect to the commercial use and, in some cases, export of encryption algorithms, whether hardware or software-based. The main goal of these rules is to prevent the availability of powerful bulk-encryption processing capabilities, as these could be used for criminal purposes. As a result of these rules, the implementation of encryption in payment systems is often restricted to financial data only.

Data *integrity* and *authentication* (including non-repudiation) are achieved by using DES, triple-DES and public key algorithms such as RSA, and by applying well-known hashing and MAC algorithms, such as MD-5, SHA-1 and RSA.

Safe storage of secret keys

In addition to choosing appropriate cryptographic algorithms, payment system designers must ensure that secret and private cryptographic keys are stored safely and that tampering or eavesdropping will be detected or will result in the destruction of the remaining data. In practice, these keys are stored in security modules in host computers, payment terminals and payment modules, and on the IC chip.

Key management

Experience with key management is common amongst many payment system designers and operators as a result of their experience in executing and designing key management for point-of-sale environments. The relevance of sound key-management principles lies in the creation of extra barriers to attackers. For example, periodic changes of security keys (or different generations of keys) limit the usefulness of particular keys that an attacker might derive from an exhaustive key search.

SECURITY ASSESSMENT

It can be stated that, in theory, cryptography allows payment systems to be designed in a safe, secure and fleckless way. In order to breach the security of those systems, an attacker would need to steal the keys, to try all combinations of possible keys in sequence, or to apply the results of cryptanalysis using the discovered weaknesses or characteristics of the algorithms to break the algorithm. Depending on the key size used, the amount of time needed to succeed in such an attack can be calculated.

In symmetric cryptosystems, it would take a substantial effort to break a system with 56 bit keys such as DES, but this can be accomplished quite easily with special hardware. The cost of the special hardware is not insignificant, but is certainly not beyond the means of organised criminals, major companies and governments. Keys with 64 bits can probably be broken by major governments, and will be within the reach of organised criminals, major companies and other governments within a few years. Keys with 80 bits may become vulnerable in the near future. Keys with 128 bits will probably remain resistant to brute-force attacks for the foreseeable future.

The key lengths used in asymmetric cryptography are usually much longer than those used in symmetric ciphers. With asymmetric algorithms, the problem is not to determine the correct key, but to derive the matching secret key from the public key. In the case of RSA, this is equivalent to factoring a large integer that has two large prime factors. In the case of some other cryptosystems, the problem is equivalent to computing the discrete logarithm modulo for a large integer (which is believed to be roughly comparable to factoring). Other cryptosystems are based on yet other techniques.

For an RSA cryptosystem, a 256 bit modulus is easily factored by a computer user with average experience and resources. Keys with 384 bits can be broken by university research groups or companies; 512 bit keys are within the reach of major governments. Keys with 768 bits are probably not secure in the long term. Keys with 1,024 bits and more should be secure for a number of years unless major algorithmic advances are made in factoring; keys of 2,048 bits are considered by many to be secure for decades.

In practice, cost considerations will lead to design decisions with respect to the choice and application of certain cryptographic safeguards. These design decisions are not aimed at achieving the highest theoretical level of security, but at providing a level of security such that the cost of attacking a system will substantially exceed the possible financial gain to an attacker. The Task Force has not observed essentially different opinions among suppliers on issues such as the weaknesses and

strengths of particular algorithms, necessary key lengths for symmetric and asymmetric algorithms, and the best key-management practices.

Although from a theoretical as well as a practical point of view it is possible to design sufficiently safe payment systems, it is critical to evaluate the actual execution of the security measures, in addition to the design of the systems. Such evaluations must take place periodically, as advances in cryptanalysis might expose weaknesses in the applied algorithms over time. Furthermore, it must be stressed that not only technical and cryptographic issues are a concern in these evaluations. The organisational and procedural design choices and execution of procedures must also be considered.