EUROPEAN CENTRAL BANK

ISSUES PAPER

E-PAYMENTS IN EUROPE – THE EUROSYSTEM'S PERSPECTIVE

16 September 2002

EXECUTIVE SUMMARY

Eurosystem's first investigation into retail e-payments

This paper presents a first comprehensive investigation by the Eurosystem into retail e-payments, i.e. payments that are initiated and processed electronically. The overview given by this paper, which concentrates on e-payments used in retail e-commerce, indicates that manifold approaches and solutions have emerged recently. The legislation relevant to e-payments and e-payment security initiatives and solutions has likewise developed considerably in the past years. The Eurosystem is now starting to define its policies concerning e-payments. The aim of this paper is to initiate a dialogue with the market on how the Eurosystem could contribute to this field. The Eurosystem is organising a conference on e-payments on 19 November 2002 where some of the issues presented in this paper will be further discussed.

Move towards e-invoicing, e-payments and e-reconciliation

Common to all initiatives covered in this paper is the automation of the payment transaction. E-invoicing, which focuses on the automation of the billing process between the payer and the beneficiary, has experienced only limited customer adoption so far. E-reconciliation, which involves the electronic communication of balance and payment information from the payment provider to the beneficiary for book-keeping purposes, is already widely used between large companies and their banks, and is to an increasing degree available also to smaller companies. In e-payments, which focus on the relationship between the payer and the payment provider, an abundance of heterogeneous initiatives have emerged. These consist of traditional payment instruments that have been adapted for e-commerce, and new payment instruments and services that are still in their early adoption phase. Credit cards have, however, remained the single most used payment instrument on the internet.

Legal and security concerns are being addressed

One of the main obstacles to the development of e-payments is the lack of customer trust in these initiatives. An adequate legal structure and security framework could foster the use of e-payments. The European Commission has developed a legal framework related to e-commerce, which consists of a Directive to ensure the free movement of online services, a Directive covering the issuance of e-money, and a Directive for the creation of e-signatures. Central in these Directives is the country-of-origin principle, allowing mutual recognition of licences and supervision between countries in the European Union. To address the security concerns, several security initiatives have been developed by market participants. Encryption based on asymmetric keys, often referred to as public key encryption, has been one of the most debated techniques to address security needs. One of the most relevant challenges of public key encryption is the building of the Public Key Infrastructure (PKI) that

needs to be in place to ensure trust in large, open user groups and to manage the keys. So far PKI has faced hurdles in achieving widespread acceptance.

Eurosystem focuses on improving efficiency...

Pursuant to its statutory responsibility "to promote the smooth operation of payment systems", the Eurosystem sees its role in the area of e-payments mainly in the promotion of the efficiency and security of the associated instruments and the related systems. The Eurosystem aims to fulfil this public policy role for the time being by acting as a catalyst for developments in the field, e.g. by engaging in a dialogue with market participants, by providing analysis and a forum for debate and by taking into account business needs in its policies. The public experiences the largest benefits from e-payments when the various participants in the payment process (payer, payee and the payment providers) operate seamlessly together. It is therefore important for e-payments that standards for interoperability across national borders and systems are developed and implemented. These standards should also tackle issues related to the interoperability of security schemes. Ideally, these standards should be discussed and the efforts co-ordinated on a global level. The Eurosystem is currently investigating the implementation of existing standards throughout the e-payment process and areas where further standards would be needed to enable full straight-through processing (STP) from payment presentment to payment reconciliation.

...and security of e-payments

While the security of e-money and e-payments can be improved by the implementation of more stringent and consistent security requirements, these can also make the systems more costly for consumers, merchants and payment service providers, thereby limiting the adoption and efficiency of the services. Because of this possible trade-off between security requirements and efficiency, the right balance between these two factors must be found. With a view to meeting this objective, the Eurosystem could together with market participants develop general security guidelines, security objectives and possibly more detailed security requirements. The Eurosystem's security objectives for e-money systems could also serve as a basis for other e-payments.

Do retail interbank systems need to adapt?

E-payments may impose special requirements on interbank payment systems. Requirements for efficient interbank settlement could include the choice of message standards that are compatible with other parts of the electronic payment process, operational procedures such as increased real-time processing, and standardised information in the payment message to allow automated reconciliation of payments at the beneficiary level. These and other possible requirements of e-payments should be taken into account in the development of retail clearing and settlement infrastructures. The Eurosystem will closely follow the creation of pan-European systems from this perspective.

1. Introduction

E-commerce[1] transactions enabled by (or transacted through) the internet or wireless networks are growing rapidly in the European Union (EU). The e-commerce market in Europe was valued at €14 billion in 1999 and €95 billion in 2000, reflecting growth of 680%.[2] A continued growth of e-commerce in Europe is also expected for the next years.

The increasing use of new communication technologies and the need for specific payment mechanisms for e-commerce have created opportunities for new intermediaries to facilitate the sending and processing of payment instructions. At the same time, banks have also developed new means to access customer accounts and to originate payments. In this paper, these new payment mechanisms and services are generally called electronic payments (e-payments). Although all payments that are initiated and processed electronically are considered to be e-payments, this paper only considers e-payments for retail e-commerce.

The Eurosystem, in its statutory task of promoting the smooth operation of payment systems, could play a key role in furthering the efficient and secure operation of e-payments – a prerequisite for their increased adoption. This paper provides an overview of the main initiatives and developments in the field of e-payments in Europe, and evaluates possible implications of these developments for the payment system policies of the Eurosystem. The report is divided into five sections. Section 2 elaborates on market initiatives regarding e-payments. Section 3 briefly describes the legal framework and Section 4 discusses technical security. Section 5 concludes with policy considerations.

The paper is not intended as an exhaustive survey of all developments in the field, or of all the issues that surround these developments. As with any paper handling current topics in a field changing rapidly in both technological and organisational terms, some parts of the paper are likely to become out of date quickly after publication.

---

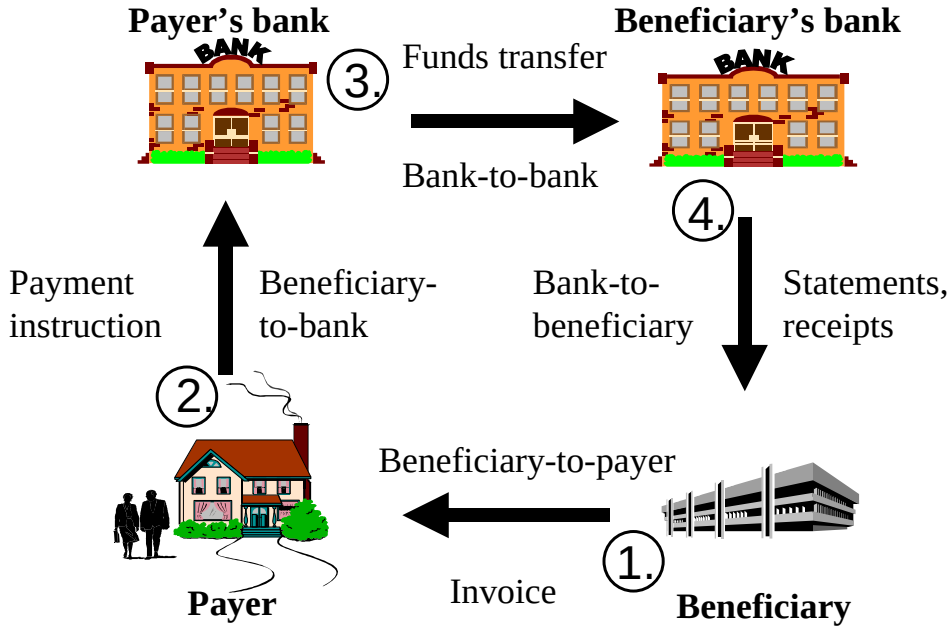
1 The OECD's broad definition of e-commerce is used in this paper, i.e. "An electronic transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organisations, conducted over computer-mediated networks. The goods and services are ordered over those networks, but the payment and the ultimate delivery of the good or service may be conducted on or off line" (see OECD Information Technology Outlook 2002, p. 131).

2 Information published by the European Commission (Just Numbers 2001 - Numbers on Internet use, electronic commerce, IT and related figures for the European Community, January 2001).

2. E-payment circle and e-payment initiatives

Figure 1 below presents, in a stylised form, the payment circle, corresponding to a normal credit transfer made to pay an invoice. Until rather recently, most of the processes in the circle were conducted manually and electronic transmission of invoice, payment and settlement information was not as widespread as it is today. Developments in technology have made it possible for banks and new entrants into the payment service market to increase the efficiency of the traditional payment process, and to provide new payment mechanisms for e-commerce. This section takes stock of such initiatives.

Figure 1: Payment circle for credit transfers[3]



Developments in the first link in the payment circle, the communication of the payment information by the biller to its customer, are discussed in Sub-section 2.1. This sub-section also discusses developments in the relationship between the biller and its bank. Electronic communication of payment and balance information for reconciliation purposes has, for a few decades, been a reality for large corporations, but has only lately become available to smaller companies as well.

In the second half of the 1990s, the internet and mobile phones became widely available and made remote provision of payment services directly to customers commercially viable. At the same time, a growing need for payment mechanisms for e-commerce on the internet manifested itself. The developments in the traditional payment instruments as they were adapted to use on the internet or

[3] Adapted from H. Leinonen, "Re-engineering payment systems for the e-world", Bank of Finland Discussion Paper 17, 2000.

mobile networks and the emergence of new innovative payment services are discussed in Sub-section 2.2.

The communication of payment information between banks and the interbank settlement of the payments has largely taken place electronically in Europe for a good time already. This paper does not discuss topics related to developments in this area, but merely points under the policy considerations (in Sub-section 5.5) to some issues related to e-payments that should be considered in the development of interbank payment systems.

2.1 E-invoicing and e-reconciliation

In recent years, the electronic transmission of invoices to customers has attracted much attention. There are several ways in which this can be done in practice, but generally the e-invoices are sent either directly to the customer or to a payment service provider, which collects the e-invoices of several beneficiaries for the customer. The latter service is also called Electronic Bill Presentment and Payment (EBPP) and the service provider that operates the EBPP system and presents the bills to the customer is called a "consolidator". The consolidator can be a general information service provider or a financial institution. In some countries, banks have become increasingly interested in providing EBPP services. In an EBPP service, customers can centrally receive all e-invoices, including any relevant information, and have e-payment facilities available to initiate the payment. The merchant can provide to the consolidator either only the summary of the bill ("thin consolidation") or all details of the bill ("thick consolidation"). In the case of thin consolidation, the customer generally has to establish a link with the merchant's website for the details of the bill.

Companies can benefit from e-invoicing and EBPP through reduced billing and payment processing expenses, as well as improved customer service and direct marketing opportunities. EBPP could also allow the integration of billing into cash management and accounting procedures. Customers can benefit from e-invoicing and EBPP through better control over payment timing and archiving, and through cost savings.

The use of EBPP has, however, remained rather limited so far. Many companies and financial institutions are waiting for the market to reach critical mass before offering electronic invoices to their customers. The lack of customer demand, the diversity of technological standards and the lack of support by financial institutions could be identified as the other reasons for the limited market adoption.

Some EBPP solutions also include accounts receivable matching features, i.e. automated reconciliation based on remittance information (e-reconciliation). Generally, the matching is done through a unique payment reference number generated by the application, which enables the association of invoice details with the payment information received from the payment service provider. In several European countries, such reference numbers have already been used on paper invoices for a long time.

2.2 E-payment initiatives

A wide range of initiatives for e-payments over the internet and wireless networks have been developed by a large number of payment service providers, including financial institutions and new providers of payment services comprising technology and telecommunication companies. The new payment service providers offer their products either directly to customers (positioning themselves between the banks and their customers) or to financial institutions (providing the technical know-how and/or operational facilities). This paper looks at e-payments from two perspectives. A distinction is made between e-payment initiatives based on traditional payment instruments (Sub-section 2.2.1) and new means of payment and payment services (Sub-section 2.2.2).

2.2.1 Existing payment instruments adapted to the internet

The following sub-sections present an overview of the methods and techniques, which have been developed to adapt the traditional payment instruments for use over the internet.

Credit cards

Credit cards allow customers to make purchases and/or withdraw cash up to a prearranged ceiling. The credit that is granted is either settled in full by the end of a specified period, generally a month, or can be settled in part, with the remaining balance extended as credit. The former arrangements are sometimes called delayed debit cards, but for the sake of simplicity both variations are called credit cards in this paper. Credit cards are used in the EU in 5-6% of all non-cash transactions, and they are the most popular non-cash payment instrument in Greece and Luxembourg.[4]

Credit cards are also widely used for making payments over the internet because they currently have some advantages over other payment instruments. Credit cards are internationally known to customers and accepted by merchants. They are also easy to use on the internet, as only the credit card details need to be sent to the beneficiary in order to effect a payment. Over the years, the credit card industry has automated card transaction processing by implementing clear standards and routing systems (including card numbering principles) in international payment networks. Therefore, the cost of cross-border credit card payments is generally not very high for the consumer compared with other means of payment, such as credit transfers or cheques. However, the increase in credit card fraud over the internet has raised security concerns for credit card companies, merchants and consumers.

In the early stages of credit card use on the internet, the card number and expiration date were simply sent by the payer to the beneficiary via the internet in unencrypted form. Credit card details could be intercepted during transmission and used illegally for purchases or for the creation of fake credit cards.

---

[4] "Payment and securities settlement systems in the European Union (Blue Book)", Addendum, ECB, July 2002. Figures for the year 2000.

In addition, credit card details along with purchase information were often stored unprotected on server computers, from which they could be obtained by hackers.

Several standards have been developed and initiatives launched in recent years to allow safer transmission and storage of credit card information. These include inter alia SSL (Secure Sockets Layer), SET (Secure Electronic Transaction), Visa 3D Secure and MasterCard SPA. The complexity of and lack of interoperability between the different initiatives has, however, hampered customer adoption of technologies other than SSL. These initiatives are discussed in more detail in Sub-section 4.3.

Another approach to ensuring confidentiality of credit card numbers has been the use of "virtual" credit card numbers. These one-time-use credit card numbers are generated when the user is linked to his/her bank server on the internet. This technique avoids the need to disclose the real credit card number online. The merchant does not have to modify its card acceptance system and cannot even distinguish a virtual credit card number from a real one. The card issuer recognises the number as being linked to the customer's credit card account and authorises the purchase. "E-carte Bleue" from Carte Bleue in France is an example of an initiative using this technique.

Credit transfers

A credit transfer is an instruction from the payer to his/her bank to transfer on demand deposits of a certain value to the beneficiary's account. Credit transfers are the most widely used payment instrument in the EU (32% of all non-cash payments[5]) and are the most common payment instrument in Sweden, Finland and Austria. Gradually credit transfers are also becoming a payment instrument for e-commerce. The majority of banks in Europe already provide e-banking applications to their customers with which online credit transfers can be initiated.

Some banks also encourage their customers to use credit transfers for purchases from online shops by providing additional e-commerce facilities. For example, customers can initiate a payment in real time directly from the merchant's website by selecting credit transfer as the payment method (e.g. by clicking on the bank's logo) and accepting the bill that appears on the computer screen. The customer is then directed to the bank's website to execute the payment and returns, after successful completion of the transfer, back to the merchant's site for order details. Such services are offered, for example, in the Nordic countries and Austria. Some payment service providers also offer their customers online malls with e-payment schemes administered by the banks. These payment arrangements require prior agreement between the merchant and the bank and between the customer and the bank (i.e. the merchant has to accept the bank's payment solution and the customer has to have access to the e-banking facilities of the bank). For the time being, most agreements are strictly national.

---

[5] Ibid.

Debit instruments

Debit instruments allow the payer to have purchases directly charged (debited) to funds on his/her account at a deposit-taking institution. A distinction is made between three types of debit instruments: direct debits, debit cards and cheques.

- Direct debits

Direct debits are pre-authorised debits on the payer's bank account that are initiated by the beneficiary. Direct debits are currently often used for recurring payments, such as utility bill payments (e.g. for water, electricity and telephone usage), or for one-time payments where there is no direct contact between the payer and beneficiary. Of all non-cash payments in the EU, 25% are direct debits. Direct debits are most popular in Spain, Germany and Austria.[6]

In a direct debit payment, the beneficiary sends the order to the payer. The payer fills in the form (i.e. acknowledges the beneficiary's claim) and sends it back to the beneficiary. The beneficiary verifies the form and forwards it to the payment service provider, which collects the direct debit from the payer's account.

Direct debits can in some countries also be used on the internet. A direct debit is initiated in a similar way to a payment by credit card. The difference is that the bank account number (and any routing information) is used instead of the credit card number and that the funds are debited from the account individually at the latest within a few days. Direct debit schemes share the same difficulty as credit cards in user authentication on the internet. They are usually also restricted to use within a specific country, which makes direct debit less suitable for cross-border e-commerce.

- Debit cards

Debit cards provide a convenient way to present the cardholder information needed to debit the cardholder's bank account. This information is embedded in the magnetic stripe (or chip) on the back of the card. A dedicated terminal is required to read the information on the debit card and possibly to verify whether the debit card is still valid and whether the transaction would exceed usage limits set for the card. Debit cards are used in 19-20% of all EU non-cash payments and are most popular in Denmark, Belgium and the Netherlands.[7]

In some European countries, debit cards can be used in internet shops. Internet usage operates similarly to the direct debit system, but offers additional security features for payments owing to the presence of the card. The cardholder authenticates his/her identity with the help of a card reader connected to the PC. The card readers are in many cases provided by the card-issuing bank. The use of

---

6 Ibid.

7 Ibid.

debit cards for purchases on the internet is still relatively limited. Examples of debit card payment on the internet in the EU are Banxafe (Belgium) and I-Pay (the Netherlands).

- Cheques

A cheque is a written order from one party (the drawer) to another (the drawee, normally a bank) requiring the drawee to pay a specified sum on demand to the drawer or to a third party specified by the drawer. An electronic cheque follows the same principle, except that the order is in electronic format rather than in writing. Mainly payment providers in the United States have begun to offer electronic cheques (e-cheques) to allow customers to pay for purchases online. The system works with prior registration where cheque account information and the e-mail address of the payer are provided. When an e-cheque is sent, only the amount of the cheque and the beneficiary's name and e-mail address are given.

Cheques have an advantage over many other payment instruments in that they can also be used for transfers of funds between individuals. It is, however, unlikely that Europe will see the same developments as the United States. In most of the European countries, cheques do not play a prominent role, and in those countries where they are used more widely (France, Ireland and Portugal), their market share has been steadily declining and other means of payment have been developed for e-commerce. Of all non-cash payments in the EU almost 18% are still made by cheque.[8] The share of cheque payments in all non-cash payments is highest in France, Ireland and Portugal.

2.2.2 Innovative payment instruments and services

The second group of initiatives is termed as innovative payment instruments. Common to these initiatives is the use of information and telecommunication technologies that were previously not available for payment purposes.

Prepaid payment services

Several prepaid schemes have emerged in Europe for small-value e-payments. A distinction is made between three groups: (i) "e-money schemes" which were originally developed to replace small cash payments in everyday life; (ii) "personal online payment services" which were initially developed to allow person-to-person payments in online auctions; and (iii) "prepaid cards" which were developed for anonymous and small-value payments over the internet.

Common to all of these is the fact that they are based on prepayments, where the user (payer) transfers value in advance to a personalised account at a payment service provider or to a device such as a smart card. These funds can then be used to make payments to other participants in the scheme.

---

[8] Ibid.

(i) E-money schemes

Electronic money (also referred to as digital cash or electronic cash) is broadly defined by the ECB as "an electronic store of monetary value on a technical device that may be widely used for making payments to undertakings other than the issuer without necessarily involving bank accounts in the transaction, but acting as a prepaid bearer instrument" (Report on electronic money, ECB, August 1998). The electronic value is comparable to cash (although unlike cash it is not in open circulation) and can be stored e.g. on a smart card (card-based schemes) or on a personal computer (software-based schemes).

Card-based e-money schemes. Currently 25 different card-based schemes, which are generally operated by financial institutions, exist in Europe. Some card-based e-money schemes allow payments over the internet as well. On the European level, the high expectations a few years ago about the use of card-based e-money schemes have not yet been met. Card-based e-money transactions account currently for only 0.2% of all EU non-cash payments.[9] They are most popular in Belgium and Luxembourg. In e-money schemes, like in many payment schemes, there are problems in achieving critical mass. On the one hand, merchants perceive the costs of the schemes to be considerable so that many of them decide not to invest in the terminals. On the other hand, customers do not use the schemes because of the low level of acceptance by merchants.

Some examples of card-based e-money schemes are Proton (Belgium), Moneo (France), GeldKarte (Germany), MiniCASH (Luxembourg) and Chipknip (the Netherlands). Projects to foster interoperability between the different e-money schemes have been launched recently. These projects include inter alia the Ducato project (involving Banksys, Groupement des Cartes Bancaires "CB", MasterCard Europe, Interpay Nederland NV, Proton World, Sermepa, Sistema 4B and Visa International) and an interoperability project between GeldKarte and MiniCASH. However, no EU-wide roll-outs are currently planned.

Software-based e-money schemes. Software-based e-money schemes are based on tokens, which can be described as "digital coins". The tokens (or coins) are obtained from a payment service provider via the internet and are stored in a digital wallet on the user's PC. From the PC, they can then be used for making online payments on merchants' websites that accept these tokens. The merchants can redeem tokens with the payment service provider.

Most of the software-based e-money initiatives have closed down before they have been able to operate on a wider scale and as a result have existed only as pilot projects of minor importance. The last relatively large project (e-cash in Germany) was discontinued in May 2001.

---

[9] Ibid.

(ii) Personal online payment services

The growing success of auction sites on the internet has led to the emergence of payment service providers, which allow person-to-person e-payments over the internet. The schemes operate similarly to banks, i.e. customers open accounts with the payment service provider and funds on these accounts can be used to make payments. The main innovation common to these initiatives is the use of e-mails and the payment provider's website for communication between the payment provider and the users, and the ease with which new accounts are created in these schemes.

Before payers can initiate payments, they have to sign up to the scheme and make a prepayment into a bank account of the payment service provider using traditional payment instruments such as credit cards, cheques or credit transfers. When making a payment, the payer connects to the payment service provider's system (generally through its website) and submits the payment order. The payment service provider then transfers the funds on its internal accounts from the payer to the beneficiary. Generally, e-mail addresses serve as a means of identification in the systems and e-mails are sent to notify the sender and beneficiary of the payment transaction details. After the transaction has been made, the beneficiary can either withdraw the money from his/her account in the system or, if he/she wants to participate in the system, can keep the money stored in the system. Since payments within the system are executed in real time, the payment service provider does not get any float income for these transfers.

These schemes have the advantage that they allow person-to-person payments across national borders. Furthermore, the payer can pay and receive funds using an account that is funded by traditional payment instruments regardless of the physical distance. Payments can also be initiated and received conveniently (only an e-mail address is required). According to this business model, private customers are not normally charged for using the service and thus payments through it have lower costs than the services provided by banks. Also no additional hardware is required (such as smart cards and terminals) to use the service.

Several personal online payment schemes have emerged in Europe, such as MinutePay in France, Epagado.com in Spain and Cartio Micropayments in the Netherlands. The majority of these schemes are located in the United States, such as PayPal, Ecount, MoneyZap (by Western Union) and Yahoo PayDirect. Recently, some of the schemes have made alliances with banks, and some banks have started offering services based on the same concept. The latter include c2it from CitiGroup and eMoneyMail from BankOne.

(iii) Prepaid cards

In Europe, a third type of prepaid system has emerged for e-payments over the internet. In these schemes, the payer's prepaid accounts are funded through cards that are sold in kiosks and shops. A number printed on the card and only visible after scratched provides access to a prepaid account on the internet. The prepaid accounts are held in remote servers instead of being stored on the user's PC or

smart card. The value on the account can be used for e-commerce transactions of small value, although it is possible to combine the value of several cards. The advantage of these schemes is similar to the personal online payment services, i.e. that no additional hardware is required and no additional costs have to be borne by the customer. The scheme also allows for anonymous payments because no registration is needed and no bank connection or credit card details have to be sent over the internet. The acceptance by merchants is still limited. Examples of such schemes are the Paysafecard system (Austria and Germany), WWWBon (the Netherlands) and Omnipay Prepagato (Italy).

Cumulative collection services

Cumulative collection services are mainly used for the processing of smaller e-payments, which are accumulated and then paid. The payment service provider collects all transactions of registered customers and submits them periodically (e.g. at the end of each month) as a single charge to the customer. The collection procedures could be compared to the delayed payments to settle credit or delayed debit card bills. Two types of charge options can be distinguished in these schemes:

- schemes in which the transactions are settled periodically through a direct debit from the customer's bank account or via the credit card bill (e.g. in Click&Buy from Firstgate in Germany); and
- schemes in which the transactions are added to the customer's phone bill (e.g. in Click&Pay from Deutsche Telekom AG in Germany, and in the premium telephone numbers operated by telecom companies in general), or to the Internet Service Provider bill (e.g. in w-HA in France).

One benefit of cumulative collection services is that customers who do not have access to, or do not wish to use, their credit or debit cards online might be able to use these services. A further benefit is that no sensitive information needs to be transmitted in a transaction. Initiatives that add the transactions e.g. to the phone bill can be used directly by anyone receiving such bills already. Cumulative collection services may also provide a more cost-efficient facility for micro-payments than traditional payment instruments. The use of cumulative collection services has so far remained quite limited.

Payment portal services

Payment portals are payment service providers that offer a wide range of the different payment options described in the previous sections and provide merchant accounts to online retailers in general. Payment portals take care of the payment side of e-commerce operations for merchants. Merchants can redirect the customers to the payment portal's site when making online payments, where customers are given a choice between several means of payment. After successful completion of the payment, the portal notifies the e-merchant that the order can be shipped.

Examples of operational payment portals in the EU are Ogone (Belgium), Wire Card (Germany), Bibit, TWYP, Triple Deal and Global Collect (the Netherlands), MBNet (Portugal), and Debitech, Netgiro and Wallit (Sweden).

Mobile phone payments

Several initiatives have emerged for initiating e-payments from mobile phones by using short messages (SMS) or phone calls. These have also been referred to as m-payments. Most m-payment initiatives follow a simple model where the customer (payer) first identifies him/herself to the merchant by providing his/her phone number or by calling the merchant. The merchant forwards the payment and customer information to the payment service provider (e.g. through the mobile phone network). The service provider then presents the payment information to the payer for confirmation and upon confirmation (e.g. with a PIN number) records the transaction. The communication between the customer and the payment provider and/or merchant can take place through phone calls and/or short messages. The paid amount is collected by direct debit from the payer's account and credited to the beneficiary's account. Operational examples of this model in the EU include Paybox (Austria, Germany, Spain, Sweden and the United Kingdom), Mobipay and Caixamovil (Spain), Mint (Sweden) and e-Pay (Finland).

Models that offer more advanced customer identification methods incorporate this information in the mobile phone's SIM (Subscriber Identity Module) card, or are based on dual-slot mobile phones (where the phone uses a second smart card for the payment application). Such projects have been launched inter alia by "Paiement CB sur mobile" (France) and by a joint venture of Nokia, Luottokunta (the Finnish Visa issuer) and Nordea (Finland). The usage of these systems is, however, still limited.

Mobile devices are well positioned for making payments, because the penetration level of digital mobile phones is higher than that of personal computers. It is also possible to use mobile phones for all types of payments, both at manned and unmanned payment terminals, for internet payments and possibly for payments between consumers. Furthermore, mobile phones can be used both to initiate and to validate payments. Thus they could simultaneously replace the POS terminal and the payment card. Mobile devices are also constantly developing, in ways which allow them to better support m-payment solutions.

Several initiatives have been launched to promote interoperability between different solutions. These include the MOBEY forum, the Mobile electronic Transactions (MeT) initiative, the Mobile Payments Forum and PayCircle. These fora encourage the use of mobile technology in financial services and act as a link between the various standardisation bodies in the mobile telecommunication and financial industries.

2.3 Summary

Section 2 has presented an overview of initiatives in the e-payment area related to recent developments in the internet and mobile networks. Apart from the more established financial institutions such as banks and credit card companies, new payment service providers, such as telecommunication and technology companies, have also stepped in to offer payment services. There are, however, not many initiatives in which the traditional players do not play any role.

The relationship between the biller and the customer is slowly becoming more electronic. Some companies have started to offer their bills to their customers online, either directly or via a consolidator in an EBPP scheme. There has, however, not been any breakthrough in customer adoption yet. Electronic communication of balance and payment information from the payment provider to the beneficiary for book-keeping purposes (e-reconciliation) has been taking place between large companies and banks for some time already. Traditional payment providers and newcomers operating exclusively on the internet have started to provide these services to smaller billers as well.

For the relationship between the customer and the payment provider, an abundance of heterogeneous e-payment initiatives have emerged. Traditional payment instruments that have been adapted to use for e-commerce, and especially credit cards, are currently widely used for online payments. However, security shortcomings and fraud reported in the media are fuelling the security concerns of consumers and hampering the development of e-payments. The credit card sector has launched several initiatives to improve security of credit card transactions on the internet, but customer adoption has remained modest. Banks have been slower in adapting credit transfers for use on the internet. As a result, these are currently not yet widely used on the European level and most of the initiatives are local and not directed at cross-border use within the euro area. In some countries, projects have been launched to enable payments through direct debits and debit cards over the internet. These are, however, not directed towards cross-border e-commerce in the euro area.

The innovative payment instruments are still in their early adoption phase. Although statistics on their use are not readily available, it can safely be said that none of the initiatives has been adopted on a massive scale. Many of the initiatives, however, serve a particular need or a niche. Mobile phones may be well suited for vending machine or person-to-person payments. Prepaid systems on the internet have evolved from software-based e-money schemes to personal online payments e.g. on auction sites. Cumulative collection services may be well positioned for ad hoc shopping or low-value payments. Payment portals, on the other hand, could well serve the needs of cross-border e-commerce by accepting a wide array of other payment instruments.

3. Legal framework for e-commerce

This section presents a general overview of the legal framework and briefly describes the most important Directives related to e-commerce, e-payments and e-money. In the first sub-section, the Directive on electronic commerce (2000/31/EC) is described. In the second sub-section, the two e-money Directives (2000/46/EC and 2000/28/EC) and the Directive on electronic signatures (1999/93/EC) are discussed. The third sub-section lists other Directives and provisions, which are more indirectly related to e-commerce. These include the Banking Directive (2000/12/EC), the Investment Services Directive (93/22/EEC), and other provisions related to applicable law and jurisdiction, dispute resolution and consumer protection. In general, the Directives seek to increase trust in e-commerce and to promote the development of online provision of services and products (especially the cross-border provision of financial services). It should be noted that the European Commission has started a consultation process on a new legislative framework for the Single Payment Area.[10] This process may lead to the required updates of the legal instruments for which the European Commission has the right of initiative.

3.1 Electronic Commerce Directive

The E-commerce Directive (2000/31/EC[11]) is the horizontal Directive (i.e. not tailored to meet the requirements of particular sectors, such as financial services), which sets the legal basis to foster the development of e-commerce. The goal of the Directive is to ensure the "free movement of information society services between Member States":

1. "*Free movement*" implies that countries cannot impose their national laws on online services coming from other Member States.
2. "*Information society services*" is a synonym for online services provided (products and services from e-commerce activities)
3. "*Between Member States*", i.e. limited to countries of the EU.[12]

To achieve its goals, the E-commerce Directive addresses three main items:

1. The Directive ensures the free movement of online services through the supervision of service operators in the Member State where they are established ("*country of origin*" principle[13]). For

[10] "A Possible Legal Framework for the Single Payment Area in the Internal Market", European Commission Working Document MARKT/208/2001 – Rev. 1.

[11] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal of the European Communities (OJEC) L 178, 17 July 2000, pp. 1-16.

[12] Note that international agreements would be needed to govern the relations with countries outside the EU.

example, financial services offered in Member States have to be compliant with the laws of the country of origin and benefit from mutual recognition.[14]

2. The Directive also sets up transparency measures for commercial communications and "*electronic contracting*", and ensures recognition of the legal validity of electronic contracts. Member States should allow the possibility to conclude contracts electronically.

3. It further exempts *intermediaries* (telecommunication and internet service providers) from liability in cases of transport, caching and hosting of information, in some conditions. It also encourages codes of conduct to be developed as well as co-operation between Member States and the resolution of litigation through online dispute settlement mechanisms.

A communication of the Commission on "E-commerce and financial services" issued on 7 February 2001 takes a closer look at how the Directive will apply to cross-border trade in online financial services specifically, and what changes are still necessary to establish a fully integrated European financial services market. The Commission identified further work in three areas: (i) to increase the convergence of contractual and non-contractual rules; (ii) to implement measures to increase customer confidence in internet payments and cross-border redress; and (iii) to enhance supervisory co-operation.

With the 2005 deadline for integrated retail financial services set by the Lisbon Council and the Financial Services Action Plan in mind, a debate on policies focusing on integrating retail services and making financial services more consumer-friendly was initiated during 2001. A first Communication from the Commission to the Council and the European Parliament on 7 February 2001[15] outlined the Community's e-commerce policy in broad terms and addressed the application of the Directive to the online provision of financial services. An evaluation of the E-commerce Directive was offered in the Commission's Report on E-commerce and Financial Services to the Financial Services Policy Group.[16] The Communication from the Commission to the European Parliament and the Council on Financial Services "Political challenges - June 2001 - Fourth progress report"[17] stressed the importance of moving forward in sensitive areas such as e-commerce and distance selling. A study on the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic

---

[13] The Directive defines the place of establishment as the place where an operator actually pursues an economic activity *through a fixed establishment*, irrespective of where websites or servers are situated or where the operator may have a mailbox.

[14] A Member State may derogate from the "country of origin" rule under the conditions laid down by Article 3.4. In addition, the Directive lists in an annex fields to which the rule does not apply. Contractual obligations concerning consumer contracts are excluded from this "country of origin" rule. This means that all forms of web-based financial services contracts are excluded, when provided to consumers.

[15] COM (2001) 66 final.

[16] http://europa.eu.int/comm/internal_market/en/finances/general/fspg-report.htm of 3 August 2001.

[17] COM (2001) 286 final.

payment instruments and in particular the relationship between holder and issuer of 17 April 2001 triggered a debate on whether recommendations should have a more binding effect.

On 7 May 2001, the ECOFIN Council adopted conclusions on the Commission's Communication on e-commerce and financial services in which Ministers welcomed a report of the Financial Services Policy Group on the Community's objectives in the field of electronic commerce and financial services. The report acknowledged that the E-commerce Directive has addressed the problem of the existence of legal barriers among the Member States by adopting an approach whereby, in general, the law applicable is determined by the place where the supplier is established ("place of establishment" principle). However, the report noted that a number of issues still need to be addressed, such as the following:

- how to deal with the existing derogations for certain financial services (e.g. insurance);
- the fact that there is a distinct legislative regime for online provision of services in contrast to other trading modes;
- the pressing need to identify further areas for convergence so that the Internal Market operates in the best interests of the consumer; and
- the application in practice of the derogation laid down in Article 3.4 of the E-commerce Directive.

It should be noted that the E-commerce Directive constitutes a first step in a process fostering e-commerce in the EU. Certain challenges may arise, such as the meaning of country of origin in the Directive, in the event that products/services are offered by branches and not headquarters in the EU. Further harmonisation of terms used and of underlying motivations such as taxation, insolvency, etc. is thus required.

3.2 Directives related to specific domains of e-commerce

3.2.1 E-money-related Directives

Two Directives are related to electronic money. Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions (ELMI) introduces a minimum set of harmonised prudential rules for electronic money issuance and applies the arrangements for the mutual recognition of home supervision provided for in Directive 2000/12/EC to ELMIs. This includes the safeguarding of the financial integrity and the operations of ELMIs by, on the one hand, ensuring the stability and soundness of ELMIs and, on the other, ensuring that the failure of any one individual ELMI does not result in a loss of confidence in electronic money or currency in general. The Directive further intends to create a level playing-field for the issuance of electronic money by both traditional credit institutions and ELMIs, thus ensuring that all issuers of electronic money are subject to an appropriate form of prudential supervision.

Directive 2000/28/EC of 18 September 2000 amends the Banking Directive (2000/12/EC) by also including ELMIs in the definition of credit institutions. It also extends the redeemability requirement imposed on ELMIs to traditional credit institutions. These amendments, if implemented on a national level in a consistent and harmonious way, will promote the harmonious development of electronic money issuance throughout the Community and avoid any distortion of competition between electronic money issuers, even as regards the application of monetary policy measures. The two Directives on e-money had to be implemented by 27 April 2002. However, as at August 2002 ten Member States (Austria, Denmark, Germany, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Sweden and the United Kingdom) had implemented them.

3.2.2 Directive on electronic signatures

On 19 January 2000, the Directive on a Community framework for electronic signatures (1999/93/EC) entered into force. The Member States had to implement the Directive in national legislation by 19 July 2001.[18]

The rationale for this Directive stems from the fact that divergent rules with respect to legal recognition of electronic signatures in the Member States may create significant barriers to the use of electronic communications and e-commerce. A clear Community framework regarding the conditions applying to electronic signatures could strengthen confidence in and general acceptance of the new technologies. The main objective of the Directive is twofold: first, to make sure that all Member States accept the legal validity of an electronic signature, and second, to make sure that all services relating to electronic signatures can be provided on the EU market without national obstacles.

According to the Directive, every kind of electronic authentication attached to or logically associated with the data to be signed obtains legal validity. The Directive calls such a general authentication method an "*electronic signature*". An "*advanced electronic signature*" is an electronic signature that meets some specific requirements set in the Directive.[19]

An advanced electronic signature that is based on a qualified certificate and created by a secure-signature-creation device has, according to the Directive, the same legal value as a handwritten signature. About thirty requirements need to be fulfilled in order to have this kind of signature. This paper refers to these as "*qualified*" electronic signatures.

Practically, this means that, for electronic signatures, every type of electronic authentication will be regarded as an electronic signature, as long as it is attached to or associated in a logical way with other

---

[18] OJEC L 13, 19 January 2000, pp. 12-20.

[19] Article 2 paragraph 2 of the Directive states that: "An advanced electronic signature means a signature that meets the following requirements: (i) it is uniquely linked to the signatory; (ii) it is capable of identifying the signatory; (iii) it is created using means that the signatory can maintain under his control; (iv) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable."

electronic data. Signatures created using Public Key Infrastructure (PKI) fall under electronic signatures as well. The definition of an electronic signature in the Directive does not even exclude the typed name at the bottom of an e-mail or the attachment of a scanned signature to a document. Furthermore, the Member States shall ensure that advanced electronic signatures based on a qualified certificate and created by a secure signature creation device satisfy the legal requirements of a signature and are admissible as evidence in legal proceedings. A judge can only decline giving legal value to an electronic signature if he/she assumes the security was not sufficient to ensure trustworthiness.

The Directive is technologically neutral and is not limited, for example, to PKI (see Section 4). PKI is one technology available to implement some certification services.

According to Article 3 of the Directive (on market access), Member States shall ensure that certification services (i.e. the issuance of certificates or the provision of other services related to electronic signatures) can be provided in the EU market without being confronted with national legal barriers, such as a national licensing system. Hence, a provider of certification services is not subject to prior authorisation.

Member States are, however, allowed to introduce "voluntary accreditation schemes" to enhance the level of certification service provision.[20] This means that if a Member State wants to introduce a new electronic signature system, which is more secure than the EU electronic signatures (as defined in the Directive), it is allowed to do so. The conditions related to such schemes must according to Article 3 of the Directive be objective, transparent, proportionate and non-discriminatory. Participation in the accreditation scheme must be voluntary.

Member States shall establish a supervisory system to control the Certification Service Providers (CSPs) issuing qualified certificates and established on their territory. CSPs wishing to issue qualified certificates have to meet the conditions set out in Annex 2 of the Directive. The establishment of private bodies designated by Member States for this purpose is not excluded by the Directive.

[20] With respect to the use of electronic signatures in the public sector, Member States are permitted to make them subject to additional requirements. Typical examples are the implementation of enhanced secure electronic signature schemes for social security or taxation declaration purposes.

3.3 Related Directives and provisions

3.3.1 Directives on financial services

The Banking Directive (2000/12/EC) of 20 March 2000 provides for a European passport for credit institutions to offer services and to set up branches in other Member States. It also enables credit institutions to access foreign payment systems located in the EU not only through branches established in the country, but also by remote access without physical presence, provided they accept the conditions of the respective systems.

The Investment Services Directive (93/22/EEC)[21] allows the cross-border provision of investment services. It is currently under review. It allows trading platforms (e-marketplaces), regulated as investment firms or regulated markets, to have remote access from other Member States. Once implemented, a minimal harmonisation of the national legislation will be achieved.

3.3.2 Applicable law, jurisdiction and dispute resolution

The Regulation 44/2001 of 22 December 2000 (the "Brussels Regulation")[22] replacing the Brussels Convention on jurisdiction and the recognition and enforcement of judgements in civil matters determines the jurisdiction. It entered into force on 1 March 2002. As a general rule, the competence of the court lies in the country of residence of the defendant's domicile. However, the competence of the court lies in the residence of the consumer, if the contract has been concluded in the Member State of the consumer's domicile, or if the company directs its activities to the consumers.

The Rome Convention of 1980 on the law applicable to contractual obligations determines inter alia the law applicable to financial services contracts.[23] In general, parties are free to choose the law of their contract. If they do not, the law of the state "to which the contract has the closest connection" will be applicable.

As regards consumer contracts, a choice of law made by the parties shall not have the result of depriving the consumer of the protection afforded to him/her by the mandatory rules of the law of the country in which he/she has his/her habitual residence, in particular if in that country the conclusion of the contract was preceded by a specific invitation addressed to him/her or by advertising, and he/she had taken in that country all the steps necessary on his/her part for the conclusion of the contract.

A Recommendation of the Commission of 30 March 1998 on Alternative Dispute Resolution/Online Dispute Resolution (ADR/ODR) addresses the principles that extra-judicial dispute settlement bodies

---

[21] OJEC L 197, 6 August 1993, p. 58.

[22] OJEC L 12/1, 16 January 2001.

[23] It is noted that the adoption of a Regulation replacing the Rome Convention is envisaged.

should respect. Further to a Council Resolution of 3 April 2000, a network of national bodies for the extra-judicial settlement of consumer disputes is being set up, the EEJ-NET (European Extra-Judicial Network). For financial services, FIN-NET (Financial Services Complaint Network) was launched in February 2001, complementing the EEJ-NET by providing a specific redress network for disputes involving financial services.

3.3.3 Consumer protection

The Council reached a common position on the proposal for a Directive on distance marketing of financial services on 19 December 2001.[24] The political agreement provides that Member States may not adopt provisions other than those laid down in the Directive in the fields it harmonises, unless otherwise specifically indicated in this Directive. The political agreement also recalls that the Directive is to be applied in conformity with the E-commerce Directive, the latter being applicable solely to the transactions it covers. The Directive does not affect the applicability to distance marketing of financial services of the Community or national law governing the freedom to provide services or, where applicable, the host country control and/or authorisation or supervision systems in the Member States where this is compatible with Community legislation. Nor does the Directive affect the applicability of the above-mentioned Brussels Regulation or the applicability of the Rome Convention.

The political agreement covers the information to be provided to the consumer prior to the conclusion of the contract (regarding the supplier, the financial service, the contract and redress procedures), the right of withdrawal, payment for the service provided before withdrawal, payment by card and also unsolicited services and communications. The agreement provides some mechanisms of notification to the Commission of provisions which Member States adopt in the field governed by the Directive. Pending further harmonisation, Member States may maintain or introduce more stringent provisions on prior information requirements. However, these additional measures must be notified to the Commission. National rules may be imposed by Member States on suppliers established in a Member State which has not yet transposed the Directive and which has no obligations corresponding to those provided for in the Directive.

A Directive concerning the processing of personal data and protection of privacy in the electronic communications sector was adopted on 12 July 2002.[25] It aims to update Directive 97/66/EC of 15 December 1997 (on data protection in the telecommunications sector) to cover new and foreseeable developments in electronic communications services and technologies, so that a high level of

---

[24] OJEC C 58 E, 5 March 2002, p. 32 ff.

[25] OJ L 201, 31/7.2002, p. 37.

protection for personal data and privacy continues to be guaranteed for all electronic communications services regardless of the technology used.

3.4 Summary

The legal framework for e-commerce addresses the problems which could arise from online trade and payments in different legal, contractual and judicial systems across the EU. The framework consists of a horizontal Directive to ensure the free movement of online services and two vertical Directives covering the issuance of e-money and the legal validity of e-signatures. Central to these Directives is the country of origin principle, which allows mutual recognition of licences and supervision between countries in the EU. In addition, there are related Directives and provisions, which were not designed specifically for e-commerce, but which are nonetheless relevant for developments in e-commerce by defining the competence of the court and the applicable law, and by regulating the provision of cross-border banking services. The Commission has recently initiated a discussion on a new legislative framework for a Single Payment Area.

4. Security of e-payments

Security concerns regarding e-payments are one of the most commonly cited reasons by the public not to use these payment instruments.[26] This section focuses on the way security is implemented in e-payments by providing an overview of symmetric and asymmetric cryptography and analysing their merits and applications. In addition, some issues concerning PKI are presented. Annex 1 elaborates on some PKI initiatives and on interoperability initiatives related to PKI schemes.

4.1 Security components of e-payments

The overall security of e-payments and online transactions in general comprises several components. Some of the most important are:

- Availability: the instrument provides efficient and timely response and has adequate capacity in order to support acceptable performance, and is able to recover quickly from disruptions.
- Authenticity and authorisation: the instrument has appropriate measures to authenticate the correct identity and authorisation of customers using the service, and to make sure that all transactions are legitimate.

[26] According to the OECD Information Technology Outlook 2002, surveys conducted in the Nordic countries and Japan show that security concerns and uncertainty concerning payments are some of the main barriers for the development of e-commerce (pp. 150-152).

- Integrity: the instrument has the appropriate measures to protect data integrity in e-payment transactions. This means that e-payment-related information in transit or in storage cannot be altered or deleted without authorisation.
- Non-repudiation: the instrument uses transaction authentication methods that promote non-repudiation and establish accountability for e-payment transactions. Proof that a message has been sent and received is provided to protect the sender against false denial of receipt by the recipient, and to protect the recipient against a false claim by the sender that the data have been sent.
- Confidentiality: the instrument takes the appropriate measures to preserve the confidentiality of relevant e-payment information. Key information should not be disclosed in such a way that it can be viewed or used by those unauthorised to do so.

Many of these security aspects can only be achieved by combining different techniques, typically by using encryption technologies with proper organisational measures. So far, the organisational measures have been the main obstacle to these requirements being successfully implemented on a large scale, while the technologies to meet these requirements have been available for some time.

A further important aspect of any e-payment scheme is the issue of liability. The security of a scheme (and consumer trust in it) can also be enhanced by an appropriate division of liability between the consumer, the merchant and the payment service provider, e.g. on the basis of their responsibilities in securing the transaction. Providing security in e-payments is not only an issue of technology, but also of a valid business model that is accepted by customers and not too costly for its users.

4.2 Technologies to meet security requirements

The technologies to secure e-payment transactions can be broadly classified under two different types of methods: symmetric and asymmetric encryption. The following sections provide a rough outline of some of the concepts involved in these two types of cryptography. The outline is not intended to be exhaustive, but only to facilitate an understanding of some of the main issues involved.

4.2.1 Symmetric encryption

In symmetric encryption (secret key cryptography), a shared secret key is used for both encryption and decryption. Symmetric cryptographic algorithms are comparatively fast as they employ fairly simple mathematics and therefore can also quickly encrypt and decrypt large volumes of data. The security requirements in terms of non-repudiation, authentication, data integrity and confidentiality can be met using symmetric encryption, although, for the first two, supplementary measures are normally needed.

However, the proper fulfilment of those requirements depends on the set-up put in place to share keys between different parties. It requires every person that communicates with another person to have a different key for each of the recipients. Therefore, the entity that supplies the keys must make sure that two different recipients do not share the same key and must provide a secure way of transmitting the

keys to the users. Furthermore, when the size of the communication network increases, the number of key exchanges needed between persons in the network rises much faster than the number of participants in the network.[27] For example, if four people want to exchange encrypted information using symmetric encryption, each one needs to exchange a bilateral secret key with the correspondent counterpart. This means that in total six secret keys will need to be exchanged to allow secure communications between all pairs of these four people. With 40 people in the network, already 780 bilateral key exchanges are necessary.

The Data Encryption Standard (DES) and its variants (e.g. the stronger Triple DES), and the International Data Encryption Algorithm (IDEA) are the two most commonly used symmetric encryption standards. The Advanced Encryption Standard (AES) is a new symmetric encryption standard.

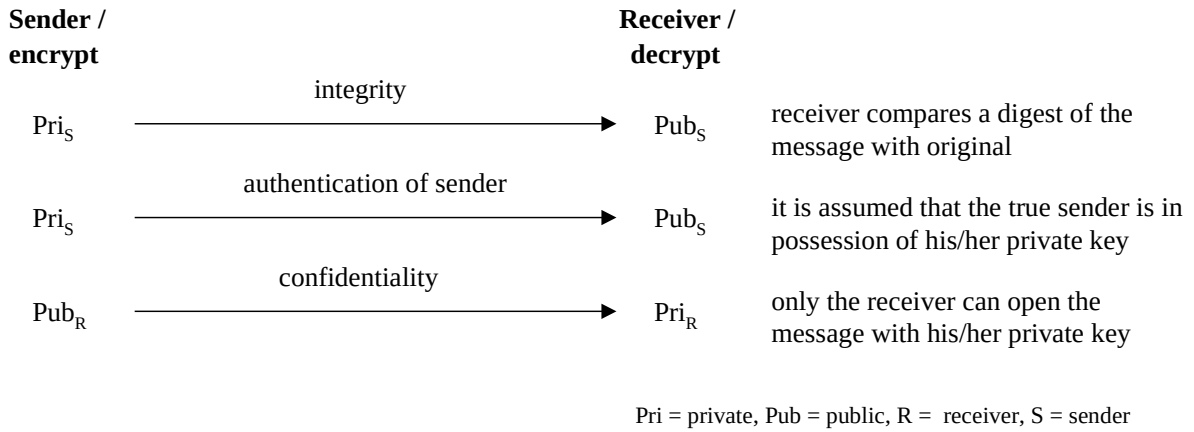
The major disadvantage of symmetric encryption thus lies in the secure exchange of secret keys. Symmetric encryption might not be efficient and secure if it has to be used to exchange information among a large number of people. Asymmetric encryption techniques could address these shortcomings.

4.2.2 Asymmetric encryption

Asymmetric encryption (Public Key Cryptography, PKC) reduces the key distribution problem by splitting the encryption and decryption keys into a mathematically associated unique key pair, one being public and one being private. The owner must carefully protect the private key, but the public key corresponding to that private key is freely distributed. In asymmetric encryption, data encrypted with the public key can only be decrypted with the private key. Conversely, data that has been encrypted with the private key can only be decrypted with the corresponding public key. The major advantage of asymmetric encryption over symmetric encryption is that fewer key exchanges are needed (as the private key does not need to be shared, just transmitted once to its owner). Therefore, asymmetric techniques are especially suited to the security requirements of communication in open networks.

[27] The number of bilateral key exchanges is n*(n-1)/2, where n is the number of participants in the network.

Figure 3: Public key encryption



As with symmetric encryption, the security features described above can also be achieved by public key encryption (see Figure 3). Public key encryption allows for *electronic signatures*, which can ensure the *integrity* of the message that is sent and the *authentication* of the sender of the message.[28] The electronic signature is typically formed by encrypting a digest of the message (i.e. a block of data calculated from the original message) with the sender's private key. The digest together with the original message is sent to the receiver. The receiver decrypts the digest with the sender's public key and compares it with the value he/she calculates from the original message him/herself. If the values do not match the message has been altered. If the two values are the same, integrity of the message is very likely to be guaranteed.

The receiver can also authenticate the sender with good confidence, because the message can only be opened with the public key of the sender and the sender should be the only person possessing his/her private key. *Non-repudiation* is a principle by which the receiver of a message cannot deny having received that message, nor the sender of having sent it, and whether this principle can be applied depends on the legislation and the degree of confidence with which it can be assumed that the private key of the sender was in fact in the sender's possession.

Although public key encryption can achieve *confidentiality* of transmitted information through the encryption of the message with the receiver's public key, usually symmetric techniques are used for ensuring confidentiality. This is explained by the fact that asymmetric key cryptography is for this purpose more resource-intensive owing to its more complex mathematics and that it is by far slower than symmetric algorithms.

---

[28] Normally in transactions (e.g. on the internet) it is more important that the party to which the payment is made can be authenticated (*server side authentication*) and the need to authenticate the user (*client side authentication*) is not as great. In e.g. online banking applications on the other hand both parties have to be authenticated. This might be done through different techniques, a weak form being the use of user names and passwords.

To make sure that the security features are in fact achieved in larger scale implementations, a trusted third party is required. A PKI implementation requires the institutions providing services related to key management (issuing, publishing and revoking) and ensuring that the public key is associated with its rightful owner. A PKI consequently requires a combination of PKC and an organisational infrastructure to provide the full set of security services. There are several different implementations of the model, depending on the company/organisation providing the service and the platform the service is run on (e.g. internet or mobile network). Some examples of PKC and PKI in payment applications and some considerations relevant for PKIs that are used for payments are discussed in the next sections.

Generally, the infrastructure is composed of a Certification Authority (CA), a Registration Authority (RA), and a facility responsible for storing public keys and lists of revoked keys (Directory Services). One institution can (and normally does) perform several of these three functions. Such institutions are referred to in this paper as Certification Service Providers (CSPs).

The role of the RA is to verify the identity of the person or organisation (i.e. it checks whether the individual/organisation is who it is claiming to be) before the key pair is issued. The strictness of the check depends on the intended use of the key pair and the security requirements. The RA can, for example, require less detailed information from an individual, which uses certificates for private identification purposes, than from corporate entities, which use certificates for payment applications.

The key pair is issued by the CA on the basis of the information obtained from the RA. Depending on the required security level, the private key can be stored e.g. on a smart card, on a SIM card or on the hard drive of a computer, and the public key is published in the Directory Services. The Directory Services are a publicly accessible repository for storing and retrieving public keys and other information relevant to them. The CA also revokes keys and publishes lists of revoked keys.

In many cases a PKI consists of a *trust hierarchy*, where CAs higher in the hierarchy prove the identity of CAs lower in the hierarchy. If the receiver of an encrypted message receives a certificate from an unknown CA, it can develop trust in that CA by validating the CA's certificate with the superior CA that issued it. The CA at the top of the hierarchy is generally called the *root CA*.

4.3 Examples of asymmetric techniques in payments

4.3.1 Secure Sockets Layer and Transport Layer Security

Secure Sockets Layer (SSL) is a communication protocol, which is currently the most widely used method that employs PKC. More specifically, it is used to establish a secure connection between a client and the server that only lasts for the life of the session (and is therefore called session-oriented protocol). SSL provides confidentiality and integrity of the data exchanged between the customer and

the merchant. It was originally developed by Netscape and later adopted by the Internet Engineering Task Force (IETF)[29] as a general standard. It is used also in many online banking applications and in credit card transactions over the internet. Virtually all browsers are SSL-enabled, meaning that they authenticate the *server* to which the user is connected and encrypt the data that are being exchanged. Normally the *user* is authenticated using other methods, such as a user name and a password. SSL itself does not support non-repudiation. A newer version of SSL was named Transport Layer Security (TLS).

4.3.2 Security initiatives by credit card companies

Secure Electronic Transaction (SET) is a debit/credit card application protocol based on PKI. It was specifically developed in the early 1990s by the credit card companies and vendors for use in financial transactions over the internet. SET provides consumer and merchant authentication, confidentiality and integrity of data, and enables non-repudiation. Furthermore, it provides not only for a protocol for the encryption of credit card numbers as they cross the internet, but also for hiding card details from some of the parties to the transaction (such as the merchant). The SET protocol is based on a hierarchical authentication referred to as "trust chaining". The SET root certification authority issues certificates to payment card brands to enable them to issue certificates to their members, cardholders and merchants. SET has, however, failed to gain widespread market acceptance owing to the lack of incentives for the participants to join the system, relatively high costs and complexity of implementation.

In 2001, the major credit card companies developed new authentication standards for online transactions. Visa launched 3-D Secure (also referred to as "Verified by Visa") and MasterCard introduced Secure Payment Application (SPA). The systems are technically very different, but both

Visa and MasterCard use SSL to ensure integrity and confidentiality of information during a transaction. In the 3-D Secure scheme, the customer has to provide a user name and password to authenticate him/herself at a central server operated by Visa. The PKI-based certificates are only used for the transaction flow between the merchant and the issuer (and not for the other participants). MasterCard SPA uses a user wallet for authentication of the cardholder. The issuer determines the method to access the wallet, e.g. either by password, smart cards, digital certificates, biometrics or other access control technologies. Both schemes are customer-friendly, but it is too early to indicate whether these solutions will gain momentum.

---

[29] The IETF has defined a number of Requests For Comments (RFCs are an archival document series of the IETF, including inter alia proposed, draft and actual standards) to specify a secure architecture for the internet, where PKC is used as an important element.

4.3.3 Common Electronic Purse Specification

A card-based e-money application protocol, the Common Electronic Purse Specification (CEPS),[30] has been developed to allow interoperability between such schemes. It has been designed to enable the use of card-based e-money online, with multiple currencies, and a higher level of security through the use of PKI. In 2001, several European card companies and associations[31] launched projects to implement and validate card-based e-money schemes based on CEPS. However, plans for a wider implementation have not yet been announced.

4.3.4 PKI in mobile networks

An important technological development for e-payments and e-commerce is the use of the mobile phone as a terminal to access a wide range of services (termed as mobile commerce or m-commerce). Mobile phones can already be used to access financial services, via short message (SMS) or Wireless Application Protocol (WAP)[32] services. Furthermore, newer technologies for mobile communication, i.e. GPRS and UMTS,[33] are allowing wider access to internet-based commercial services. There have been several initiatives to create a PKI for mobile communication, but no breakthrough has yet been made.[34] It cannot be excluded, however, that the PKI model could play an important role in the future in securing m-commerce and m-payments.

---

[30] CEPS is managed by a consortium called CEPSco, jointly owned by PWI (Belgium), Zentraler Kreditausschuss (ZKA, Germany), SERMEPA (Spain) and Visa. Interpay (the Netherlands) and Groupement des Cartes Bancaires (France) are also involved in the management of CEPS.

[31] Banksys, MasterCard Europe, Interpay, Proton World, Sermepa, Sistema 4B and Visa International, Centre de Transfers Electroniques (CETREL), ZKA, Groupement des Cartes Bancaires and Société Européenne de Monnaie Electronique (SEME).

[32] WAP is an open, global specification that enables mobile users with wireless devices to access the internet.

[33] General Packet Radio Service (GPRS) is a packet-based technology that enables high-speed (115 kilobits per second) wireless internet and data communications. Universal Mobile Telecommunications System (UMTS) is the third generation of mobile networks standardised by ETSI. It will provide data speeds of up to 2 Mbps. GPRS is generally considered as a bridge to UMTS.

[34] The Wireless Application Forum has defined a number of specifications to enable secure communications and trust relationships. In particular, a Wireless Application Protocol Public Key Infrastructure (WPKI) definition was published in April 2001, with the aim of reusing existing PKI standards for WAP applications.

4.4 Considerations about Public Key Infrastructure

In the following sub-sections, some considerations related to PKI are presented from legal, technical, organisational and interoperability perspectives.

4.4.1 Legal considerations

Different national laws could have implications for certificate authorities and their liabilities and for the deployment of PKI technology in general. In addition, the dispute resolution framework (for when problems occur with the use of the certificates) could differ across national legal systems.

The E-signature Directive defines qualified electronic signatures (see Sub-section 3.2.1) in a functional, non-technical way. Due to the technology-neutral approach of the Directive, work needs to be carried out on setting standards for fulfilling the requirements. The European standardisation bodies are working on technical standards, which comply with the Directive and can easily be implemented in technical solutions (the so-called EESSI Initiative). Furthermore, the E-signature Directive does not specify how it should be ensured that the CSPs act in a prudent manner and leaves this aspect to the Member States. In addition, the effectiveness of the electronic signature process depends upon the reliable association of a public-private key pair with an identified person. In the absence of clear requirements and procedures for these requirements to be met, an RA might refrain from prudently verifying the identities of persons to whom they issue certificates for e-payments.

4.4.2 Technical and organisational considerations

A PKI model requires good implementation and prudent operation, which are essential to guarantee the proper use of certificates and proper verification of a certificate's validity. Some considerations that need to be addressed are:

- How is the trustworthiness of the institution that provides the public key certificates (the CA), or of the institution that authorises other certification authorities, ensured?
- How carefully does the CA verify the identity of the applicant?
- How are the private signing keys protected from misuse? These keys may be stored e.g. on PCs that are subject to attacks. Under some jurisdictions, responsibility for the private key remains with its rightful owner, even in the event that it is stolen and misused.
- How is the security of the Directory Services ensured? Attackers could e.g. add their own public key (under an imaginary name) to the directory or a public key in the name of somebody else (e.g. a company).
- How is tampering with keys detected? Are they then revoked? Can the revocation be retroactive? (i.e. can a certificate holder deny having made some signature in the past?)

- How can the robustness of an e-signature certification scheme be measured? All applications do not require the same degree of security. Some solutions may, however, be unsuitable for payment and financial applications.

4.4.3 Interoperability considerations

The development of PKI is, at the moment, focusing on building proprietary solutions that could, by involving a large number of participants, become de facto standards in specific environments. These private PKI solutions reflect corporate business needs (such as Identrus for financial services) and will implement different PKI architectures, security policies and cryptographic tools to meet specific needs.

It can be expected that in the future efforts will move to address the need for interoperability among different proprietary solutions developed by competitors in the same corporate business (as already observed for smart card technology). Large companies may have a competitive advantage as they will be able to impose a "proprietary PKI application" simply because they have a large number of customers and hence possible counterparts. In the banking sector, large banks could be the leading force and might impose solutions on the smaller players and their customers.

A wider interoperability of e-payment PKI schemes would facilitate consumer adoption because of increased scope. Such increased interoperability would mean that the critical mass needed for successful implementation of an e-payment PKI would be likely to be achieved sooner. Interoperability would also increase efficiency by limiting the need for investment by both users and merchants. Some work to achieve interoperability is already under way. Annex 1 provides an overview of the different models for achieving interoperability among CAs and lists interoperability initiatives and national PKI schemes.

4.5 Summary

The main obstacles to any security infrastructure are related to establishing the appropriate organisational framework needed to complement the technical implementation. This is true for both symmetric and asymmetric encryption technologies. It is also obvious that when secure communication needs to be established between several parties, symmetric encryption might not be efficient, as the distribution of bilaterally shared secret keys can become a very burdensome and risky task. However, although asymmetric encryption simplifies key distribution, it does not solve the problem completely. One of the most relevant challenges with asymmetric encryption is the establishment of the infrastructure needed to provide trust and to manage the keys. This infrastructure that combines cryptographic tools with the organisational framework is known as PKI.

PKI initiatives are being implemented throughout the EU to ensure security of all types of electronic transactions over the internet. At the same time, different implementations of PKI and different

regulatory frameworks can be observed across Europe. From a European perspective, two questions are important. Firstly, will PKI become a dominant method for securing e-payment? Secondly, if this were to happen, how could interoperability of the different schemes be ensured without compromising the desired level of security? In addition to user acceptance, legal, technical and organisational considerations are important to answer the first question. PKI does require a relatively complex infrastructure with relatively high costs. If simpler and cheaper solutions are available, those may come to dominate the market. PKI developments in other sectors (such as digital IDs provided by public authorities) might also provide security elements for e-payments.

5. Policy considerations

5.1 Introduction

The tasks of the Eurosystem in the area of payment systems and instruments aim at the promotion of their security and efficiency, notably to safeguard the monetary policy transmission mechanism and to contribute to the maintenance of systemic stability and public confidence in the currency. This part of the paper discusses the rationale for Eurosystem involvement in e-payments from these perspectives, and outlines work that the Eurosystem envisages carrying out. This paper also aims to initiate a discussion with market participants to identify together the areas where Eurosystem involvement would be most beneficial.

As regards e-payments, the Eurosystem's focus will at least initially be on the promotion of security and efficiency of e-payment systems. With regard to these goals, the Eurosystem sees at present its role as that of a catalyst for change, with the aim of achieving a balance between public policy objectives and business needs through a dialogue with market participants. Issues related to the efficiency and security of e-payments are discussed in Sub-sections 5.2 and 5.3.

E-payments in their current form do not have a significant influence on the functioning of the monetary policy transmission mechanism. Some issues related to this are, however, of importance and are discussed in Sub-section 5.4.

The further adoption and development of e-payments are closely linked to the development of the retail payment infrastructure in general. Sub-section 5.5 discusses the relationship between e-payments and traditional interbank payment systems.

5.2 Efficiency of payment instruments

Rationale for Eurosystem interest

Issues related to the efficiency of payment instruments are of major importance, especially in the euro area with the creation of a single payment area. Moreover, the cost of a nation's payment system can be substantial. Technological innovations such as e-payments can reduce this cost and thereby increase welfare.

The largest benefits from electronic payments are experienced by the public when various parts of the payment circle operate seamlessly together. Interoperability across different systems and across national borders, and standards allowing straight-through processing (STP) in the whole payment circle are important for the proliferation of e-payments in the euro area. Ideally, such standards should be discussed and the efforts co-ordinated on a global level.

Interoperability requires commonly agreed standards. However, in the early stages of development when competition for the future standards takes place, the setting of such standards may hinder innovation and give rise to "lock-in effects" that can stifle the adoption of new standards and solutions when the existing ones become obsolete or too restrictive. The formal standardisation process has occasionally proved to be too slow for the fast-moving information and telecommunication sector and instead de facto standards have emerged, some of which have been formalised at later stages.

If common standards cannot be agreed upon, the existing investments in non-interoperable technologies can make the adoption of new standards more costly in the later stages of development. An example in the area of payments is domestic payment standards, which make cross-border payments within the euro area costly and the development of an interoperable infrastructure time- and resource-consuming. While payment infrastructures on the domestic level can be highly developed and efficient, inefficiencies exist in cross-border payments where different domestic payment standards are in use.

There are, however, examples (such as the GSM standard in the field of mobile communication) which show that, if standards can be agreed upon early on, cross-border interoperability will be enhanced and the adoption increased.

Envisaged future work

The Eurosystem endeavours, in co-operation with standardisation bodies and market participants, to help strike the right balance between competing and commonly agreed standards. Banks have traditionally dominated the provision of payment services. The emergence of new providers of payment services, such as telecommunication operators and companies offering payment services on the internet, creates new challenges. If various service providers were to be responsible for different parts of the payment circle, as to a large extent is the case, standards for the interfaces between the entities in the payment circle would be welcomed.

When looking at the beginning of the payment circle, the standards for the electronic communication of invoice information (e-invoices and EBPP) between the beneficiary and the payer are not yet widely deployed. Concerning the communication between the payer and his/her bank or the payment service provider, some elements for the electronic presentation of payments exist. The new e-payment initiatives streamline payment input and validation, and the payment form standard, the ePI (electronic Payment Initiator), is being finalised by the European Committee for Banking Standards (ECBS) to facilitate this.

For the interbank leg of payments, the work carried out by the Eurosystem on interbank retail infrastructure is of relevance.[35] The way in which the special requirements of e-payments should be taken into account in the development of the interbank settlement and clearing infrastructure is discussed separately in Sub-section 5.5.

There are however no European standards for the final leg in the payment circle between the beneficiary and his/her bank or the payment service provider concerning the synchronisation of invoice and account information ("reconciliation") at the biller level. In online business, where the full benefits are reaped in end-to-end STP, this is clearly a shortcoming that unnecessarily increases the costs of cross-border e-commerce.

The Eurosystem will start to investigate the implementation of existing standards and areas where further standards would be needed to enable full STP from payment presentment to payment reconciliation.

5.3 Security of payment instruments

Rationale for Eurosystem interest

The Eurosystem's interest in the security of e-payments stems from two sources. Firstly, the Eurosystem as part of its oversight activities is concerned about the security of all payment instruments used by the public, which may have a bearing on public confidence in the currency. A perceived or real lack of security of specific payment instruments might lead to a loss in confidence in the instrument and could, in the extreme case, have a negative impact on the functioning of the monetary system, e.g. if reverting to other means of payment is difficult or if the loss of confidence spills over to these other instruments as well. Secondly, the Eurosystem, in its role as a catalyst promoting the adoption and efficiency of payment instruments, will also have to take into account their security. Security concerns regarding e.g. online payments are one of the most commonly cited reasons by the public for not using online payment instruments. Major incidents experienced by the

[35] See e.g. "Towards an integrated infrastructure for credit transfers in euro", ECB, November 2001, "Improving cross-border retail payment services – Progress report", ECB, September 2000, and "Improving cross-border retail payment services in the euro area – the Eurosystem's view", ECB, September 1999.

public in the use of new and possibly more efficient payment services could lead to a delayed adoption of these or their abandonment.

Envisaged future work

The involvement of the Eurosystem in enhancing the level of security could span from issuing general security guidelines to setting technical requirements. Three alternatives are presented for discussion below:

(i) The Eurosystem could develop general security guidelines or best practices together with market participants. These guidelines could serve as guidance in the development of e-payment schemes and as an agreed checklist or benchmark for systems with acceptable security features.

(ii) The Eurosystem, has drawn up a list of security objectives for e-money schemes, with a focus on technical security. These security objectives are based on the "Common Criteria" (CC) framework, an internationally agreed and standardised framework for the specification of security objectives and requirements. In particular, the CC framework provides the structure for specifying and evaluating the technical security features of IT products and systems. At this stage, the Eurosystem has focused only on the security objectives, being aware that a complete assessment within the CC framework would also include security requirements and an evaluation process. Further investigations will be undertaken in order to determine how this work on the security requirements may best be conducted. An open issue is whether it would be feasible and advisable to extend the CC methodology used for e-money schemes to e-payments more generally. Some central banks are already investigating the technical and organisational security features of e-payment initiatives and are considering issuing a list of "security referentials" for the technical features of e-payments (not necessarily based on the CC framework).

(iii) Other concepts, such as the elaboration of detailed requirements for technical security and interoperability, could also be considered. A label could be introduced for the banking industry to ensure interoperability and include optional (enhanced) levels of security requirements for specific domains, such as e-payments.

While the security of e-payments can be improved by more stringent security requirements, these can also make the system more costly and complex for consumers, merchants and payment service providers, thereby diminishing the adoption and efficiency of a given service. Because of this possible trade-off between security and efficiency, the right balance between these two must be found in a joint effort by the Eurosystem and market participants.

Looking more specifically at PKI, common technical and organisational security requirements and procedures that would ensure that those requirements are met by the payment service providers are currently not available. Furthermore, the contractual arrangements between customers and service

providers to protect the customer against fraud and financial loss might not always be solid or might work to the disadvantage of the customer. Interoperability between the various schemes remains an open question. Interoperability of PKIs, especially in terms of accepting certificates issued by another CA and verifying their validity online, would benefit the development of e-payments in the euro area.

The Eurosystem envisages starting a discussion with market participants about whether there is a need for Eurosystem involvement in the aforementioned or other areas.

5.4 Monetary policy aspects

Monetary policy considerations relate more to electronic money than other e-payments. An article[36] published in the ECB Monthly Bulletin discusses these issues in more detail and therefore only the three main issues regarding electronic money and monetary policy are summarised here.

First, there is a need to safeguard the role of money as the unit of account for economic transactions. The redeemability requirement for electronic money, laid down in Community legislation (see Sub-section 3.2.1), is important to ensure that the development of electronic money does not endanger the function of money as a unit of account.

Second, the effectiveness of monetary policy instruments might be affected by a widespread adoption of electronic money. However, the above-mentioned legislation foresees that the ECB may impose reserve requirements on issuers of electronic money. Furthermore, as long as some form of ultimate recourse to central banks remains, the ability of central banks to influence money market interest rates will be preserved.

Third, the emergence of electronic money may have repercussions on the information content of monetary indicator variables. This said, the ECB has the ability to collect data and compile statistics on electronic money.

As a conclusion and taking the previous points into consideration, the ECB does not expect its ability to maintain price stability to be endangered by the development of electronic money.

5.5 Interbank payment systems

Rationale for Eurosystem interest

The Eurosystem's oversight activities notably aim to maintain systemic stability by containing the exposure of payment systems to systemic risk, i.e. the risk that a failure of one participant in the system creates a chain reaction of failures that could undermine the stability of financial institutions and markets. The focus for oversight activities aiming to ensure systemic stability is on payment

[36] "Issues arising from the emergence of electronic money", ECB Monthly Bulletin, November 2000.

systems. All large-value payment systems in the euro area are considered to be systemically important and some retail payment systems are of actual or potential systemic importance.

The majority of the new initiatives do not change the interbank settlement process, but use current systems, where settlement is effected through banks in the interbank payment systems. Therefore, these innovative payment services face efficiency constraints, as they have to be built on the existing systems – especially in cross-border payments. The implications of the increased use of innovative technologies in the interbank payment process should, however, be investigated in more detail.

The settlement in retail systems is currently based on batches and netting, without synchronisation of payment and settlement information.[37] A push towards real-time settlement can be expected, because the expectations of the public for real-time payments are increasing and information and telecommunication costs are decreasing.

The main driver for the changes in the interbank payment process is the demands that customers make on their banks. Their demands are increasing owing to developments in other fields (e-mail, sharply reduced costs of telephone calls, etc.). Bank customers' increasing expectations and competition from the newcomers, which are able to offer cheaper and faster payments (at least at the cross-border level), will put pressure on banks to enhance their internal processes. Likewise, interbank payment systems need to react to the changing needs as well.

Envisaged future work

The question of how existing retail interbank settlement systems can adapt to better meet the requirements of e-payments arises. This is true for both systems run by central banks and systems run by private entities. The requirements of e-payments should be kept in mind in the development of the retail clearing and settlement infrastructure in Europe, including the choice of message standards and operational procedures. Issues that could be considered might include standardised information in the payment message to help automated reconciliation at the beneficiary level as discussed in Sub-section 5.2 on efficiency of payment instruments, or the direct participation of non-banks in the clearing arrangements. The Eurosystem will also closely follow the developments in the creation of a pan-European automated clearing house from this perspective.

[37] Unlike in real-time gross settlement (RTGS) systems where these are simultaneous.

ANNEX 1 PKI schemes and their interoperability

Currently, several CSPs are available to provide security services using PKI and are acting as CAs. There are up to a hundred CSPs operational worldwide. Many of these have been founded by financial institutions either nationally or internationally to provide services to a specific community. Some are private and some are backed by public authorities. The following paragraphs present some European initiatives:

An overview of national initiatives in the EU

Many national PKI-based initiatives have emerged in Europe, some of which are listed below.

In Belgium, the major banks together with the national debit card operator (Banksys), the interbank network for corporate financial services (Isabel) and the Belgian Post Office Group have founded the ECERTIO company, which focuses on the production of digital certificates. The clients of these partners will be able to execute e-banking, e-commerce and e-government transactions using their ECERTIO certificate.

In Finland, several PKI solutions have been developed. Electronic Identification Cards are issued by the Population Register Centre. The cards identify the user and can be used for some government and communal online services. They also serve as an official travel document for Finnish citizens in European countries. Also SET, EMV (Europay, MasterCard, Visa) and SIM solutions based on PKI are used in Finland. In a joint initiative, banks, retailers and the post office have founded a company called Certall for the provision of PKI services to its shareholders (currently exclusively banks).

In France, there are several initiatives using PKI technology such as the online declaration of VAT and some social taxes. PKI initiatives are being developed in the health sector (i.e. the Sesame/Vitale and CPS programmes) to facilitate healthcare-related payments. The transposition of the Electronic Signature Directive (which is in its ultimate phase) and the governmental action plan for the information society are encouraging private initiatives. Currently, there are about ten CSPs in France providing security services using PKI and acting as CAs or RAs (such as Certinomis, which is a national mail company, and Certplus).

In Germany, several initiatives employing PKI technology have been introduced. Examples of this may be found in the banking industry, the health sector, tax consultancy, administrative authorities and trade and industry. Following the transposition of the EU Directive on electronic signatures into national law on 16 May 2001, a root authority was founded by the *Regulierungsbehörde für Post und Telekommunikation*, the German authority which regulates the telecommunications market and postal services. At the moment, 14 CSPs are accredited and one CSP has announced its qualified certificate service. In what is known as the “Bund Online” e-government initiative, the German Government announced its intention to use PKI-based technology within administrative authorities and for electronic communication with the general public and trade and industry. This initiative uses a

standardisation of PKI services and security measures for electronic communication like e-mail or file transfer. Moreover, the Teletrust Association founded the European "Bridge-CA" initiative in 2001 for the purpose of connecting existing PKIs in a secure and flexible manner and to avoid cross-certification. The Teletrust Association was established as a non-profit organisation in 1989 with the aim of promoting the trustworthiness of information and communication. Participants in Bridge-CA come from the banking industry, administrative authorities and trade and industry (see www.bridge-ca.org).

In Italy, efficient co-operation between private and public entities is enabling an adequate interoperability level, even in the absence of the traditional hierarchical approach. The 12 Italian operating CAs, the Italian public administration IT authority and the Banca d'Italia have agreed on "Interoperability Guidelines" that solve the problem of interoperability at the national level.

In Norway, the PKI has been developed as a national scheme (involving government, banks, etc.), allowing personal identification and banking information certificates to be stored on one smart card. The advantages of a nationally based implementation are numerous: (i) greater trust of the users/citizens; (ii) better interoperability and lower costs further enhancing interoperability; (iii) simplification and streamlining of related procedures and processes; (iv) co-operation among involved parties; and (v) more integrated services.

In Spain, several e-signature initiatives have been undertaken, allowing for a more rapid and efficient execution of both financial and non-financial operations. Initiatives involving public bodies are, on the one hand, promoting safe and efficient e-communication between citizens and the public administration to allow them to electronically complete several administrative procedures (e.g. ID renewal, data consultation, claim presentment, electronic tax return presentment, etc.). There have also been private initiatives, such as the establishment of ACE (Agencia de Certificación Española), which offers PKI-based corporate security solutions to its shareholders (i.e. the three network providers for card payments in Spain). Their certificates are either based on X.509 standards or SET specifications, thus allowing for a potential interoperability with other CAs located in other countries.

In Sweden, PKI schemes are used for banking (e.g. the Internet Bank of Svenska Handelsbanken) and for identity cards. One identity card service is offered jointly by the major banks and BG COM and another is offered by the Swedish Post Office and Telia. Currently, banks in co-operation with the tax authorities are working on PKI-based solutions for transactions with the government.

Private cross-border initiatives

In September 1999, a group of banks and banking associations representing more than 800 banks around the world set up the **Global Trust Authority** (GTA), an international organisation based in Belgium that aims to facilitate secure cross-border transactions. GTA is a limited liability, not-for-profit organisation.

GTA is seeking to provide an environment where transacting parties have confidence that each party can be authenticated, irrespective of the type of transaction mechanism being used, and that there is a redress facility if a loss arises as a result of a failure in the identification and authentication mechanisms. The aim of GTA is to enable participating trading parties to establish a trusted electronic trading relationship.

GTA will operate as the root CA (i.e. the highest CA in the system), which issues public key certificates to the CAs under the GTA umbrella (generally its founders). It will operate a Directory Service and maintain a Certificate Revocation List (CRL).

Another large-scale initiative is **Identrus**, which was created by eight large financial institutions in April 1999.[38] At the end of 2001, the initiative had more than 50 partners. The Identrus solution is designed to enable legally enforceable e-commerce transactions within a technological and operational framework where all the participants can manage risk and establish a uniform global system of participation rules and operating procedures.[39] These rules and procedures will bind both parties to any transaction and, if needed, provide a well-defined dispute resolution process and recourse mechanism.

Like GTA, Identrus establishes: (i) a policy including standard systems, practices, processes and risk management policies; (ii) a root certification to enable participating financial institutions to certify the identities of their corporate customers; (iii) a repository to maintain a real-time database of all underlying participation certificates in order to provide real-time validation services; and (iv) system operations to manage the audit requirements for adherence to a set of uniform rules, standards, contracts and business practices. Identrus has strict eligibility rules and high participation costs, meaning that only about 300 banks in the world would be able to operate as level-one participants.

Initiatives to improve interoperability

PKI initiatives can be categorised as follows:

- Single CA: this is the simplest PKI model. It is, however, not scalable and does not easily meet all the requirements of users/applications.
- Hierarchical CAs: in this approach, a superior-subordinate link is established between CAs, leading up to a root CA. The root CA does not issue certificates to users, but only to subordinate CA
- Meshed CAs: this approach is based on peer-to-peer relationships between CAs. The links enable cross-certification

[38] These include ABN AMRO, Bank of America, Barclays, Chase Manhattan, Citigroup, Deutsche Bank, Bankers Trust and HypoVereinsbank.

- Bridge CA: in this approach, CAs are linked by a "bridge entity" that is not a root CA but connects different trust domains.

Each of the above configurations has both advantages and disadvantages. It is not within the scope of this paper to enter into the technical and operational details of these configurations. A summary of major European projects to enhance interoperability is presented below.

ICE-CAR

ICE-CAR[40] is a project founded by the European Commission. The aim of the project is to foster the development of European security technology for the purpose of securing the growing use of open networks, such as the internet, and to promote the availability of technically compatible and interconnectable PKIs. Within ICE-CAR, a **EuroPKI Top Level (Root) Certification Authority** has been established. It is a non-profit organisation established to create and develop pan-European PKI. Currently the national CAs of Austria, Ireland, Italy, Norway, Slovenia and the United Kingdom participate in the project.

European Electronic Signature Standardisation Initiative (EESSI)

EESSI was launched by the European Information and Communications Technology Standards Board (ICTSB),[41] with the support of the European Commission in 1999. It plans to develop a number of technical, procedural and quality standards for electronic signature products and solutions compliant with the Directive on electronic signatures. The main role of EESSI is to co-ordinate the work of the industry and the European standards bodies (European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI)) to provide an agreed framework for an open, market-oriented implementation of the Directive. In December 2000, it released "Policy requirements for certification authorities issuing qualified certificates" and it recently published guidelines on conformity assessment by CAs against technical standards. CEN/ISSS[42] is responsible for the part of the EESSI work programme dealing with quality and functional standards for signature creation and verification products, as well as quality and functional standards for CSPs. A workshop was launched on electronic signatures in December 1999, which is currently in the process of finalising a first set of security requirements for certificate management. The Electronic Signature Infrastructure (ESI)

---

[39] Identrus requires the private key to be stored on a smart card in order to protect it from hackers.

[40] Interworking Public Key Certification Infrastructure for Commerce, Administration and Research.

[41] The ICTSB is an initiative from the three European standards organisations to co-ordinate activities in the field of the information and communications technologies (ICT).

[42] The Information Society Standardisation System (ISSS) of the CEN.

Working Group of ETSI SEC[43] is in charge of the telecommunications standardisation activities related to the EESSI work programme.

PKI-Challenge

PKI-Challenge is a two-year project founded by the European Commission and organised by EEMA (which is a European forum for electronic business). It started in January 2001 and aims to provide a solution for interoperability between PKI-related products and to develop specifications and best practices.

[43] The Security Committee (SEC) of ETSI.

ANNEX 2 List of relevant websites

ACTION	www.project-action.org
BBS - Bankenes Betalingssentral (Norway)	www.bbsas.no
bezahlen.at	www.bezahlen.at
BGC - Bankgirocentralen (Sweden)	www.bgc.nu
Bibit	www.bibit.com
Billpoint	www.billpoint.com
Bolero.net	www.bolero.net
c2it	www.c2it.com
Carte Bleue	www.carte-bleue.com
CEN/ISSS	www.cenorm.be/isss
Commission - ISPO	europa.eu.int/ISPO
Cyber-Comm	www.cybercomm.fr
Debitech	www.debitech.com
e-faktura	www.e-faktura.com
e-giro	www.e-giro.se
e-Pay	www.aldata.fi/acprojektit/epay
ECBS	www.ecbs.org
ecount	www.ecount.com
EESSI	www.ict.etsi.org/eessi/EESSI-homepage.htm
E-MoneyMail	www.bankone.com/presents/emoneymail/home/
Epagado	www.epagado.com
ePSO	epso.jrc.es
ETSI SEC	www.etsi.org/sec/el-sign.htm
EUR-Lex	europa.eu.int/eur-lex/en
MasterCard Europe	www.mastercardeurope.com
EuropeProfile	www.europeprofile.com
Firstgate	www.firstgate.de
I-Pay	www.i-pay.com
ICE-CAR	ice-car.darmstadt.gmd.de
ICT	www.ict.etsi.org
Identrus	www.identrus.com
IETF	www.ietf.org
Internet Fraud Complaint Center	www.ifccfbi.gov
Interpay	www.interpay.nl
ISO	www.iso.org

Just Numbers (Commission)	www.drecommerce.com/justnumbers/
Luottokunta	www.luottokunta.fi
MBNet	www.mbnet.pt
Mint	www.mint.nu
Mobey Forum	www.mobeyforum.org
Mobile Payment Forum	www.mobilepaymentforum.org
Mobipay	www.mobipay.com
MonayZap	www.moneyzap.com
Net900	www.in-medias-res.com
Netcraft	www.netcraft.com
Netgiro	www.netgiro.se
netpay	www.netpay.at
Ogone	www.ogone.be
Orbian	www.orbian.com
Paybox	www.paybox.net
Paymaster	www.gzs.de/de/paymaster
PayPal	www.paypal.com
PBS - Pengeinstitutternes Betalingssystem	www.pbs.dk
PKI-Challenge	www.eema.org/pki-challenge
Proton	www.banksys.be
Solo (Nordea)	www.nordea.com/eng/services/solo_internet.asp
Telepay	www.telepay.it
Visa	www.visaeu.com
w-HA	www.w-ha.fr
WWWBon	wwwbon.nl
Yahoo Paydirect	paydirect.yahoo.com

ANNEX 3 List of acronyms

Acronym	Stands for:	Referred to in Sub-section:
3D-SET	Three Domain Model for Secure Electronic Transactions	4.3.2
ADR	Alternative Dispute Resolution	3.7.2
ATM	Automated Teller Machine	2.2.1
CA	Certification Authority	4.3.2; 4.4.3
CEN	European Committee for Standardization	Annex 1
CENELEC	European Committee for Electrotechnical Standardization	Annex 1
CEPS	Common Electronic Purse Specification	4.3.3
CRL	Certificate Revocation List	4.2.2; Annex 1
CSP	Certification Service Provider	4.2.2; 4.4.1; 5.3; Annex 1
e-	electronic-	
EBPP	Electronic Bill Presentment and Payment	2.2; 2.4
EEJ-NET	European Extra-Judicial Network	3.7.2
EEMA	European forum for electronic business	Annex 1
EESSI	European Electronic Signature Standardisation Initiative	Annex 1
ePI	Electronic Payment Initiator	5.2
ELMI	Electronic Money Institution	3.6.1
EMV	Europay, MasterCard, Visa. Refers to specifications covering debit/credit cards, terminals and applications	Annex 1
ETSI	European Telecommunications Standards Institute	Annex 1
ETSI SEC	Security Committee of the European Telecommunications Standards Institute	Annex 1
FBCA	Federal Bridge Certification Authority	Annex 1
FIN-NET	Financial Services Complaint Network	3.7.2
GPRS	General Packet Radio Service	4.3.4

GSM	Groupe Spéciale Mobile, Global System for Mobile Communications	5.2
GTA	Global Trust Authority	Annex 1
ICE-CAR	Interworking Public Key Certification Infrastructure for Commerce, Administration and Research	Annex 1
ICT	Information and communications technology	Annex 1
ICTSB	European ICT Standards Board	Annex 1
IETF	Internet Engineering Task Force	4.3.1
m-	mobile-	
ODR	Online Dispute Resolution	3.7.2
PACE	Purse Application for Cross-border use in Euro	4.3.3
PKC	Public Key Cryptography	4.2.2; 4.3.1
PKI	Public Key Infrastructure	2.4; 3.6.2; 4; 4.2.2; 4.3.2/3/4; 4.4.1/2/3; 4.5; 5.3; Annex 1
POS	Point Of Sale	2.2.2
RA	Registration Authority	4.2.2
RFC	Request For Comments	4.3.1
RTGS	Real-Time Gross Settlement	5.5
SET	Secure Electronic Transaction	2.3.1; 2.4; 4.2.2
SIM	Subscriber Identity Module (mobile phones)	2.3.2; Annex 1
SMS	Short Message Service (mobile phones)	2.3.2; 4.3.4
SPA	Secure Payment Application (by MasterCard)	2.2.1; 4.3.2
SSL	Secure Sockets Layer (internet)	4.3.1/2; 2.3.1; 2.4
STP	Straight-Through Processing	5.2
TLS	Transport Layer Security (internet)	4.3.1
UMTS	Universal Mobile Telecommunications System	4.3.4
WAP	Wireless Application Protocol (mobile phones)	Annex 1
WPKI	Wireless Application Protocol Public Key Infrastructure	Annex 1