Institute for
Prospective Technological Studies
Directorate General Joint Research Centre
European Commission

Securing Internet Payments
– The potential of Public Key Cryptography, Public Key Infrastructure and Digital Signatures –

Background Paper No. 6
Electronic Payment Systems Observatory (ePSO)

January 2002

Clara Centeno

EUR 20263 EN

IPTS, Edificio Expo-WTC,
C/ Inca Garcilaso, s/n, E-41092, Seville, Spain
Tel: +34 954488281, Fax: +34 954488208
URL : http://epso.jrc.es/

European Commission

Joint Research Centre (DG JRC)

Institute for Prospective Technological Studies
http://www.jrc.es

Legal notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information.

Report EUR 20263 EN

Acknowledgements

The author would like to thank all the people and organisations that have, with their valuable contributions, helped with the elaboration of this report, with special thanks to: BankId - Norway; Banksys S.A. - Belgium; Europay International S.A. - Belgium; Odd Erling Håberget of Euro Processing International - Norway; Luigi Sciusco - Italy; Daniel Skala of CASHWARE - France; Claus Stark of Secorvo Security Consulting GmbH in Karlsruhe - Germany; Arnd Weber of ITAS, Karlsruhe Research Centre – Germany, and her ePSO team colleagues.

Abstract

The lack of trust and security has been repeatedly reported in market analysis as one of the most important factors hindering the development of e-commerce.

There is a widespread assumption that the common focus of public key cryptography (PKC), public key infrastructure (PKI), digital signatures and secure Internet payments will lead to a secure and trustworthy environment for e-commerce, as many initiatives are under way:

- the increasing use of public key cryptography (PKC) for protecting data over Internet,
- the expected implementation of digital signatures using public key infrastructure (PKI) and smart cards,
- the expected development of e-government services using PKI,
- the deployment of bank smart cards, and,
- the fast adoption of mobile devices.

However, the potential synergies can not be taken for granted. The adoption of SET, for example, has not been as successful as expected, and alternative security mechanisms such as the use of PINs or passwords seem to be gaining ground.

The role of this paper is to analyse how PKC, PKI and digital signatures can act as enablers for the deployment of secure e-payments over the Internet. To achieve this, we will first point out the risks linked to the Internet environment and the resulting security requirements for online Internet payments. Then we will analyse the concepts and security building capabilities of PKC, PKI and digital signatures and other infrastructure enabling elements such as smart cards and mobile phones. This is followed by a look at current practice, discussing the current use of these techniques in Internet and mobile payments and in other application fields such as online banking, B2B applications and e-government services.

From this, the following questions for further discussion arise:

- Is it too early for PKC, PKI and digital signatures to secure Internet payments or is PKI simply not an adequate solution?
- Should banks and governments co-operate more in the definition and implementation of PKI infrastructures?
- Should particular measures be taken to enhance consumer adoption of PKI?

CONTENTS

1 INTRODUCTION

1.1 BACKGROUND

The lack of trust and security has been repeatedly reported as one of the most important factors hindering the development of e-commerce. In the face-to-face environment of the physical market place, the transacting partners have relied upon a number of mechanisms to build security and trust. These are: physical presence at the commercial location where goods can be seen and touched, the consumer's presentation of an identification card, the use of a secret PIN code entered in a secure pin pad, the visual aspect of a payment card (brand mark, signature panel, card security elements), and the use of a hand-written signature for concluding a purchase or payment order, etc.

In order to maintain an acceptable level of security and trust when trading on open networks it is necessary not only to replace the traditional 'face-to-face' mechanisms with new digital ones but also to create new tools (digital, legal, procedural) to manage the specific risks of the open network environment where e-commerce takes place.

In this respect, there is a widespread assumption that the common focus of public key cryptography (PKC), public key infrastructure (PKI), digital signatures and secure Internet payments will lead to a secure and trustworthy environment for e-commerce. Correspondingly, many initiatives, considered complementary, are under way:

- the increasing use of public key cryptography embedded in web browsers and commercial servers for data confidentiality and integrity (SSL);
- the recent (July 2001) deadline for the EU member states for the adoption of the EU Directive on electronic signatures into the national laws;
- the recommendation of the EESSI – European Electronic Signature Standardisation Initiative – to use smart cards for the implementation of the electronic signature;
- the potential for digital signatures to replace in the Internet environment the hand-written signature used by some payment instruments;
- the banks' trials of the SET PKI based Internet payment protocol;
- the banks' current use of PKC for Internet banking services security;
- the recent (Nov 2001) Ministerial Declaration[1], where Ministers *agreed to encourage the large-scale use of electronic signature, when appropriate, for both public services and business by 2003*.

[1] Brussels, 29 November 2001, Ministers of EU member States, EFTA and countries in accession negotiations with the EU

- the expected deployment of EMV banking smart cards as a result of a technology migration from magnetic stripe based cards to reduce fraud;
- the current e-government initiatives that consider PKI for e-services security
- the fast adoption of mobile phones and their potential as the preferred user device.

However, the potential synergies can not be taken for granted. The adoption of SET, for example, has not been as successful as expected, and alternative security mechanisms such as the use of PINs or passwords seem to be gaining ground.

1.2 THE ROLE OF THIS PAPER

This sixth ePSO Background Paper is about securing Internet payments. We want to analyse how PKC, PKI and digital signatures can act as enablers for the deployment of secure e-payments over the Internet.

We will first point out the risks of the Internet environment and the resulting consumer and merchant security requirements for online Internet payments. These include data confidentiality and integrity, mutual consumer and merchant authentication, non-repudiation and limited or no liability in case of fraud. Moreover, these requirements need to co-exist with additional consumer trust building, user friendliness, costs, and interoperability requirements.

Then we will analyse the concepts and security building capabilities of PKC, PKI and digital signatures and other infrastructure enabling elements such as smart cards and mobile phones.

This is followed by a look at current practice, e.g., the current use of these techniques in Internet and mobile payments and in other application fields such as online banking, B2B applications and e-government services. This observation will show us that although these have great potential for securing Internet payments, only PKC is broadly used on the Internet to provide data confidentiality and integrity (SSL). Indeed, the banks' have proposed diverse non-PKI based security solutions because their attempts to use PKI have failed to gain widespread adoption. Other Payment Service Providers are also using alternative security techniques. At the same time, however, we observe that some payment service providers are starting to use PKI and, in parallel, PKI is emerging for mobile payments, online financial services and e-government services.

Open questions

Therefore, the following questions, which still require further discussion, arise:

- Is it too early for PKC, PKI and digital signatures to secure Internet payments or is PKI simply not an adequate solution?
- Should banks and governments co-operate more in the definition and implementation of PKI infrastructures?
- Should particular measures be taken to enhance consumer adoption of PKI?

2 SECURITY REQUIREMENTS FOR ONLINE INTERNET PAYMENTS

In an effort to understand how Public Key Cryptography (PKC), Public Key Infrastructure (PKI) and digital signatures can act as enablers for the deployment of secure e-payments over the Internet, we will start by identifying the risks linked to the Internet environment and the resulting payment security requirements, both for consumers and merchants, in the electronic market place.

2.1 RISKS IN ONLINE INTERNET PAYMENTS

Internet communication networks are insecure, and the number of security breaches continues to increase (Computer Security Institute, 2001). Examples of security breaches are:

a) interception of communications in order to copy or modify data,
b) unauthorised access to a computer or network of computers with malicious intent to copy, modify or destroy data,
c) execution of malicious code for the same purposes, and,
d) malicious misrepresentation.

As a consequence, consumers and merchants face a number of risks, when transacting through these insecure open networks. From a payment perspective, and without aiming to be exhaustive:

Consumers
- face the risk of transacting with a fake or fraudulent merchant who may bill the transaction and never deliver the goods purchased; or,
- may receive recurrent or unauthorised debits for a service subscription they never agreed to; or,
- may face the risk of having card or account data stolen and re-used for another purpose.

Merchants
- may transact with a consumer that is using stolen or fake identification and payment data which will ultimately lead to a repudiation by the rightful owner of the payment data; or,
- may face consumers denying having ordered a particular purchase which has been effectively performed.

Payment schemes statistics (Europay International, May 2001)[2] show that Internet fraud with credit cards mainly takes place at transactional sites that collect payment data and

[2] Published at 'Droit et Nouvelles Technologies' at www.droit-technologie.org

then disappear after fraudulently charging the cardholder (e.g. adult sites), or through unauthorised access to insufficiently protected payment data stored at merchant servers,.

Recent market analysis estimates that credit cards are used for 93% of Internet online payment transactions (Gartner, March 2001), of which 1.1% are fraudulent. Following current credit card rules, however, merchants are assuming liability for 90% of them (CommerceNet, May 2001).

2.2 SECURITY REQUIREMENTS FOR ONLINE INTERNET PAYMENTS

Consumer payment security requirements derive from the need to:

a) transact with trustworthy merchants,
b) receive matching offers and deliveries,
c) have a customer service or other mechanism for redressing potentially conflictive situations, and,
d) protect personal data from unauthorised access and use.

Merchant payment security requirements, however, derive from the need for payment guarantee and for protection of commercial data from unauthorised access.

Taking these user requirements into consideration, the following security requirements are generally agreed to be key components, though not sufficient on their own, in building security, trust and confidence over the Internet between two transacting parties who do not know each other (merchant and consumer): confidentiality and integrity of the information exchanged, authentication of parties, no repudiation of the transaction and liability limitation. Developing these requirements, focusing on the payment transaction and differentiating consumer and merchant needs, leads to Table 1 overleaf.

Table 1: Payment Security Requirements for Consumer and Merchant

	Consumer	**Merchant**
Confidentiality	I want to be sure that my personal data and payment details are protected from unauthorised access - during transaction processing, messages exchange, and, - after payment, at merchant's database, and from use for other purposes than the payment.	I want to be sure that my commercial information is protected (pricing, conditions, etc).
Integrity	I want to be sure that the payment information is not modified during the transaction, that what I see on the screen is what is effectively sent to the merchant and to the involved financial institutions.	I want to be sure that payment information is not modified during the transaction.
Authentication	Is the merchant the company he claims to be? Is this a trustworthy merchant?	Is the consumer who he claims to be (name, address, age, etc)? Is he using a valid payment instrument? Is he entitled to use this payment instrument for this transaction?
Repudiation / Non-repudiation	I want to be able to cancel or repudiate a transaction in case: - I did not perform it, - merchant did not provide what was agreed, - goods/services are not as they looked like, - or simply because I changed my mind.	I want to ensure that the consumer doesn't deny a transaction, after product or service delivery.
Liability	I want no liability in case of fraud, or limited liability if it was my fault.	I want no liability in case of fraud.

From the above table, we can see some symmetries but also some conflicting differences between consumer and merchant requirements, especially with respect to authentication and non-repudiation.

Authentication

The consumer need for authentication relates to building trust, that is, the need to build a transacting trust environment equivalent to that of the physical marketplace, where the shop location, the appearance of goods and personnel, and the possibility to touch and feel the goods, etc., inspire trust. The consumer need for authentication also includes the need to identify the entity towards which to address an eventual complaints.

In the virtual market place, merchant authentication is a building block for this trust building process. However, additional tools are also required such as: a contractual framework, trust marks, codes of conduct, data privacy statements, dispute resolution procedures, clear information on terms and conditions, clear pricing offer, customer service, graphical design of the web site, etc (OECD, GBDe, Egger and Abrazhevich, Klasen).

The merchant need for authentication derives from the need for a payment guarantee. The exact authentication methods and authorisation processes used to obtain this guarantee depend on the payment instrument used, which in turn is defined by the issuer in relation to the business risks associated to this instrument. The authentication can be carried out through different complementary steps: the authentication or validation of the payment instrument and its rights to be used for payment in the transaction environment and the authentication of the consumer as the entitled owner of the payment instrument. Additional steps may be required by the payment instrument in order to obtain payment guarantee such as the request for an online authorisation to the issuer. For example, an e-purse would only require authentication of payment instrument and verification of its balance, while the use of a debit card could require cardholder authentication with a PIN, and an online authorisation request to the issuer to authenticate the card and verify the funds' availability.

Non-repudiation

Where non-repudiation is concerned, consumer and merchant interests could be considered as somewhat conflicting. However, they are mostly complementary. Consumers want offer and delivery to match in terms of price, goods, delivery terms, etc, and even to be able to cancel a purchase without any specific reason (this corresponds to acknowledged consumer rights in distance selling). Merchants, in order to obtain payment guarantee, need to avoid both legitimate and fraudulent repudiation risk (that is, fraudulent orders done with stolen data for example, and real orders fraudulently denied) (Van Hove, 2001).

2.3 OTHER RELATED REQUIREMENTS

Additional tools, outside the scope of this paper, are also required in order to build consumer trust – for example, a contractual framework, trust marks, codes of conduct, data privacy statements, dispute resolution procedures, clear information on terms and

conditions, clear pricing offer, customer service, graphical design of the web site, etc – as mentioned above.

In order to ensure consumer adoption of a secure payment solution, additional requirements need to be taken into account such as: user friendliness, acceptable costs, acceptable liability terms, and a degree of familiarity with the payment instrument - i.e. one that is already used in the physical market place (Berlecon Research, 2001; Stroborn, 2001).

Finally, security requirements must also co-exist with national and cross-border interoperability requirements between buyers and merchants, across solution providers and payment networks.

3 INTRODUCTION TO PUBLIC KEY CRYPTOGRAPHY (PKC), INFRASTRUCTURE (PKI) AND DIGITAL SIGNATURE CONCEPTS

After analysing the security requirements for Internet payments, we will analyse the capabilities of PKC, PKI and digital signatures and other infrastructure enabling elements such as smart cards and mobile phones.[3]

3.1 PUBLIC KEY CRYPTOGRAPHY (PKC)

A key advantage of PKC is that it permits individuals to use two different but related keys to *authenticate* each other and maintain the *confidentiality* and *integrity* of their communications. It also allows them to digitally *sign* a document or a transaction. One key, the private key, is kept secret by the owner, while the other, the public key, can be widely distributed. The two keys are mathematically related, but an important feature is that it is computationally unfeasible to derive one key from knowledge of the other.

When two interacting parties do not know each other, PKC provides an easy mechanism for data encryption and integrity (e.g. SSL). The authentication of these parties, however, requires a trusted third party or a trust chain (e.g. PGP). A third party is also necessary to legally bind a digital signature to the signing party and to enforce non-repudiation.

3.2 PUBLIC KEY INFRASTRUCTURE (PKI)

In order to create sufficient trust for commercial transactions, that is, to use authentication and legally binding digital signatures, a trusted third party is required. This entity has to certify the validity of the certificates issued for authentication and signature, to manage these certificates (their creation, distribution, publication, revocation and renewal), to establish the contractual terms and liabilities among parties and act as neutral party in case of disputes.

The wide usage of certificates, the need for interoperability, the complexity of the technology and the secure processes reinforce the need for a common trusted third party to manage this supporting infrastructure - the Public Key Infrastructure. This encompasses secure hardware and software, security mechanisms, operational rules, organisational practices, contractual terms and liabilities, and further elements.

[3] In Appendix B, we provide a brief description of the basic concepts of PKC, PKI and digital signatures.

PKI enables additional necessary functions for e-commerce such as time-stamping, document notarisation, secure e-mail and digital proof of receipt.

3.3 DIGITAL, ELECTRONIC AND ADVANCED ELECTRONIC SIGNATURES

The term *digital signature* has been used so far in this document to refer to a signature that can be calculated by making use of hashing techniques and public key encryption to ensure the integrity of a document and to authenticate its source.[4]

The EC Directive (1999/93/EC) on electronic signatures provides the following definitions:

- *electronic signature*: data in electronic form attached to, or logically associated with, other electronic data and which serves as a method of authentication;
- *advanced electronic signature*: electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control and; (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
- *qualified certificate*: meets the Directive requirements and is provided by a certification-service-provider who fulfils the Directive (security) requirements; and
- *secure signature-creation device*: meets the Directive (security) requirements;

and stipulates that advanced electronic signatures, based on a qualified certificate and created by a secure signature-creation device, are *legally equivalent to hand-written signatures.* It also stipulates that electronic signatures are *not to be denied legal effectiveness* on the grounds that they are in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification provider, or not created by a secure signature-creation device.

Legal effectiveness can therefore also be achieved by the use of digital or electronic signatures and agreed contractual terms and conditions among parties.

However, the validity of electronic signatures has to be proved when brought to court as proof, i.e. the link between the signatory and the text signed has to be proved as well as

[4] This use is in line with the (ISO/IEC 7498-2) definition for digital signature: “data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. the recipient”.

the unaltered storage from the moment of creation until brought to court. This requirement together with the general lack of familiarity with such digital proofs in court, will, at least during the introduction phases, create a legal disadvantage for digital signatures compared to hand-written signatures (Bensoussan, 2001).

Although the EC Directive does not impose any particular technology, the expert team of EESSI has recommended the use of PKI as the most adequate enabling technology for a fast implementation of an electronic signature framework in Europe (EESSI, April 2001).

3.4 SMART CARDS AND PKI

Smart cards appear as an infrastructure enabling component for PKI, as they allow storage and protection of private keys and provide built-in cryptographic software functions to create the asymmetric key pair, generate digital signatures and encrypt/decrypt data (ensuring that the private key is never 'in clear' outside the hardware token). In addition, smart cards provide consumer authentication tools to access the private key (by use of a PIN, passwords or biometrics), and provide consumers with mobility, allowing them to perform transactions with independence of the access device (any PC, iTV, mobile phone, PDA, etc).

The following EC supported initiatives are expected to foster the deployment of smart cards for PKI:

- EESSI, which recommends the use of hardware tokens like smart cards as a way to ensure the necessary security level for digital signatures, and,
- eEurope Smart Cards, which aim is to establish smart cards in all shapes and forms as the preferred mobile and secure access key to citizen and business information society services.
- The recently endorsed specifications (May 2001) for low cost secure smart card readers by the European Committee for Standardization (CEN) as CWAs (CEN Workshop Agreements). These specifications have been drawn up by the FINREAD (Financial Transactional IC Card Reader) Consortium with a view to securing the use of IC cards issued by the banking industry for financial transactions. These specifications may boost the deployment of smart card readers. However, although the FINREAD business requirements include cost-effective adaptability to new requirements, it is not clear yet how easily these devices could securely support PKI-related functions.

In parallel, a smart-card chip equipped with a USB (Universal Serial Bus) interface hardware technology has been developed.[5] This interface has the advantage of higher diffusion in the already available electronic peripherals such as PCs and PDAs.

3.5 MOBILE OR WIRELESS PKI

Mobile devices with their embedded WIM/SIM chip (Wireless Identity Module / Subscriber Identity Module), may become an enabling component for the implementation of PKI solutions, as:

- current GSM penetration in western Europe is estimated at over 60%[6], which positions the mobile device as a preferred end user device,
- mobile phones constitute a potential device for the storage of private keys, the authentication of end-user and the generation of digital signatures, and,
- offer lower cost, mobility, high penetration and user friendliness as major advantages compared to PC-smart card-smart card reader platforms.

However, additional security, standardisation and interoperability issues still need to be resolved for the provision of wireless PKI.[7]

[5] The SMART-USB EC funded project will add to an existing security smart-card chip a Universal Serial Bus interface, and adapt it for e-commerce.

[6] GSM Europe, The European GSM Group of the GSM Association, May 2001.

[7] As pointed out by Radicchio (www.radicchio.org), The global initiative for wireless e-commerce. E.g., we observe that anti-virus experts McAfee have announced (03/2001) a special “Micro Engine” to protect WAP mobiles.

4 PKC, PKI, DIGITAL SIGNATURES AND PAYMENT INSTRUMENTS

Although global statistics point at credit cards as the most important Internet payment instrument, analysis of various national payment cultures shows that alternatives to the credit card are of importance for B2C e-commerce (Boehle and Krueger, 2001).

Analysis of how PKC and PKI could potentially increase security in the payment process for the different payment instruments used, leads to the following Table 2:

Table 2: Potential PKC, PKI and DS use for Internet payments

Payment instrument	**Security function provided by PKI**	**Options for PKC/PKI use**
Direct debit Electronic check Credit transfer	Replace current hand-written signature for payer authentication and non-repudiation.	Use of digital signature (created with bank owned PKI) & contract *Use of legal digital signatures*
Debit and credit cards	Data confidentiality and integrity; Replace current hand-written signature (or PIN) for cardholder authentication and non-repudiation; Merchant authentication.	Use of PKC (SSL) for data confidentiality and integrity Use of bank owned PKI digital signatures & contracts (SET, 3D-SET, etc) Use Payment Service Providers PKI digital signatures & contracts *Use of legal digital signatures*
Account based payment systems (e.g. PayPal)	Data confidentiality and integrity; Consumer authentication and non-repudiation; Merchant authentication.	Use of PKC (SSL) for data confidentiality and integrity Use of Payment Service Providers PKI digital signatures & contracts *Use of legal digital signatures*

From the above table, one could derive the following:

- PKI can provide additional security tools for data confidentiality and integrity and for cardholder/merchant mutual authentication,
- PKI can provide a means of replacing the current use of hand-written signatures,
- Legally recognised signatures could be used for cardholder authentication and non-repudiation, indicating a potential synergy with other market or administration sectors that may also use digital signatures.

5 USE OF PKC AND PKI IN THE B2C AND G2C FIELDS

So far we have analysed the payment security requirements and how PKC and PKI can, in theory, fulfil these requirements for different payment instruments. In this chapter, we will analyse which online payment solutions actually use PKC, PKI and digital signatures and which alternative security mechanisms are also used. We will also have a look at other applications in the consumer market and citizen segment.

The analysis will show that while PKC use has been generally adopted for payment data confidentiality and integrity (SSL), the use of PKI for B2C Internet payments is still very limited. However, we have observed emerging solutions and service providers using PKI to provide authentication and non-repudiation for online payments, mobile payments, online financial services and e-government services.

5.1 USE OF PKI FOR INTERNET PAYMENTS

5.1.1 SSL – Secure Socket Layer Protocol

In a nutshell, SSL, the Secure Socket Layer protocol developed by Netscape Communications, allows a secure connection or information 'tunnel' between the web browser and a web server, based on a combination of public key cryptography and faster symmetric cryptography for encryption/decryption.[8] This protocol provides *confidentiality* and *integrity* of data exchanged between the consumer browser and the merchant server. SSL is seen as a starting point for the definition of TLS (Transport Layer Security protocol) by the Internet Engineering Task Force (IETF), with the aim of advancing this protocol to an Internet Standard.

SSL is simple, cheap and quick to implement, and, in combination with credit card data introduced through the PC keyboard, is the most used "payment instrument" on the Internet.[9] This is reinforced by the fact that Visa International has put in place a requirement that online merchants, who accept Visa credit or debit cards, must offer encryption protection to cardholder's data by January 2002.

However, SSL only protects the link between the browser and server, but does not protect that data once it is collected by the merchant server, where most attacks take place.

[8] This is to overcome the high computational resources required by asymmetric cryptography, which make it impractical for encrypting/decrypting large amounts of data.

[9] Communication by Russ Jones from CommerceNet estimating that close to 99% of web sites that accept credit card data entry use SSL (ePSO-Forum, Sept 2001).

SSL certificates could potentially provide consumer authentication. However, this feature is not widely used by merchant servers. Instead, merchants, who are liable for fraud in these types of transactions, build fraud risk management tools such as: e-mail confirmation, consumer history database, phone call to first-time-customers, advanced payment, address validation, etc.

SSL certificates could potentially provide merchant authentication as well. However, their effectiveness is questioned by the fact that consumers today are not generally sufficiently knowledgeable about Internet security features. For example, only a small number of consumers is aware of the significance of the locker at the bottom of the screen, take active action to configure, verify, accept or reject merchant web site certificates, understand the purpose of the public/private keys stored on his PC, etc. It is also true that a number of (SSL) validation processes are done without the consumer's awareness or intervention.

SSL certificates are issued by independent Certification Authorities, and their use is governed by contractual agreement. Verisign is the leading SSL Certificate issuer in the market.

5.1.2 SET, Secure Electronic Transaction Payment Protocol

The SET Specification, is an open technical standard for the commerce industry, developed by Visa and MasterCard to allow secure credit card transactions over the Internet. The use of PKC, digital certificates and signatures creates a trust chain throughout the transaction, provides consumer and merchant *authentication*, data *confidentiality* and *integrity* and *non-repudiation* capability. However, enforcement of non-repudiation depends on the contracts established between banks and consumers and merchants under the prevailing national laws.

A particular feature of the SET protocol is that through the use specific cardholder, acquirer and merchant certificates, *payment data is protected* from merchant access. Its subsequent storage at the merchant server is thus avoided, along with the risk of it being stolen.

Certificates are issued to consumers, merchants and acquirers by their respective banks. A hierarchy of Certification Authorities exists, and the SET Root CA is owned and maintained by Secure Electronic Transaction LLC. Additional Certification Authorities are managed by the payment schemes.

Further developments (or extensions) of the initial SET protocol have taken place to support additional capabilities such as: magnetic stripe-based debit cards, online PIN, EMV based debit and credit cards, transport of CVC2/CVV2, and also the support of national solutions such as the French Carte Bancaire B0'.

Piloting of SET started in December 1997. However, although it provides all the tools for secure electronic transactions, there is, nonetheless, agreement in the market that SET has not taken off. Moreover, over half of Europe's bankers think the standard will be obsolete in two years (Lafferty, Aug 2001). The major implementation barriers identified have been:

- Lack of incentives for consumer adoption vs. complexity of use and understanding, inherent costs (smart card reader), effort and potential liability disadvantages (loss of cancellation right);
- Lack of incentives for the issuers to invest in more secure solutions that shift the liability from the merchant to the issuer bank, thereby increasing fraud cost;
- Complexity and costs of the overall implementation for the different parties;
- Technical interoperability among different vendor solutions.

5.1.3 Solutions to SSL and SET weaknesses proposed by card schemes

In order to reduce the barriers to implementing the SET protocol and resolving the security weaknesses of SSL, the card schemes, Visa and Europay/MasterCard International have proposed a number of different solutions:

- Strengthening the authentication process of the SSL-credit-card solution *with address validation* and *CVV2/CVC2 field validation* (placed in the back signature panel).
- The use of *Pseudo or Random card numbers*, where a unique card number, linked to the physical card, is generated for each transaction. This solution, in combination with SSL, provides cardholder authentication (with PIN) and avoids numbers being re-used if data is stolen.
- The use of *Virtual cards*, for Internet use only, with a reduced credit limit to reduce the fraud risk.
- The launch by VISA of the secure e-commerce initiative in June 2000 with the announcement of the *3 Domain (3D) model.* The principle of the 3D-model is that the issuer bank authenticates the cardholder, the acquirer bank authenticates the merchant, and banks authenticate each other, leaving freedom to issuers and acquirers to chose the cardholder and merchant authentication methods. There are a number of 3D-

variants: 3D-SET (also supported by Europay) for Europe and Latin America, 3D-SSL for USA, and the more recent (Aug 2001) global 3D-Secure.

In the 3D-SET model, cardholder and merchant certificates continue to be used but are held at server wallets and accessed through bank defined authentication mechanisms such as PIN or password. Visa's European Board mandated the use of SET between the issuer and acquirer banks as a required authentication protocol from October 2001.

In the other 3D variants, the 3D-model eliminates the need for cardholder/merchant mutual authentication and offers alternative - and simpler - authentication mechanisms as business relationships exist between the banks and cardholders and merchants, respectively. Within this context, the following authentication technologies are expected to gain ground:

- *Shared secret technologies,* which cover symmetric cryptography, passwords, PINs and challenge response techniques. Depending on whether the secret is unique to each pair of parties, non-repudiation is possible.
- *Biometric technologies,* where unique physiological or behavioural characteristics are used to identify or verify (authenticate) the identity of an individual. Some examples are: fingerprint, iris recognition, palm pattern, voice and face recognition, dynamic signature verification and keystrokes.

  Although from the user perspective, the reduced risk of loss or inadequate use of a secret is attractive from a liability perspective, a number of issues exist when using biometrics. Some of these are privacy, consumer acceptance, the need for and cost of hardware capture devices and storage capacity for templates. There is also a questionable level of trust (and liability level) in the uniqueness of samples, the integrity of the biometric processes and systems, the security of the sample transmission and template storage. False acceptance or false rejection may occur, revocation of compromised samples or templates may be difficult and, in case of compromise, there may be a failure to provide further service.
- *Other technologies,* which provide authentication by using a name or an electronic location, which are characteristics of the message or the machine (not of the individual), and provide therefore only a limited form of authentication. Examples of these are e-mail address, IP address and domain name

- The later announcement (Sep 2001) by Visa International of its VISA Authenticated Payment system (or "Verified by Visa"), a blend of 3D-SET, 3D-Secure and SSL based technologies. VISA Authenticated Payment is a comprehensive program that

includes technology, education, monitoring and new business rules, i.e., a liability shift to the issuer in case of fraud if the merchant uses the "Verified by Visa" service. VISA mandates European banks to support either 3D-Secure or 3D-SET by April 2003, while new liability rules will apply by April 2002 in EU and by April 2003 globally.

- The announcement by Maestro earlier this year (Feb 2001) of a new e-commerce solution for Maestro cards. This makes use of regular (vs. one-time) virtual card numbers and changing expiry dates, together with a technique chosen by the issuer for authenticating the cardholder, through a server based wallet. This solution allows e-merchants to process the transaction in the same way as credit cards. Real card data is stored at the issuer and protected from merchant access.
- The announcement by Europay/MasterCard (May 2001) of the use of *UCAF (Universal Cardholder Authentication Field)* together with *SPA™ (Secure Payment Application)* to authenticate cardholders using MasterCard or Maestro cards for online purchase. The support of UCAF/SPA is mandated for issuers and acquirer banks by April 2002. The solution is non-PKI based, uses server-based wallets and leaves at the issuer's choice to define the cardholder authentication method.

  SPA aims to bind consumer authentication, payment data and purchase order details at the issuer wallet server, by creating a unique cardholder authentication value for each transaction, equivalent to a cardholder's signature, reducing repudiation risk.

Despite the efforts made by the card schemes to propose new secure solutions to combat fraud, some questions remain such as:

- the risk that the diversity of the solutions proposed will hinder market adoption by the different actors,
- how interoperability among cardholders, merchants and indirectly between acquirer and issuers will be achieved, and,
- whether issuers will have sufficient incentives to invest in more secure solutions while taking over the liability for fraud.

5.1.4 The role of smart card based payment instruments: EMV and CEPS

The plans to migrate from magnetic stripe technology to the smart card EMV standard for debit and credit cards (roll-out expected by 2005), although initially conceived for the physical marketplace, also holds some promise for Internet payments. Indeed, it is assumed that EMV provides sufficient security mechanisms for cardholder authentication (with offline PIN validation by the card), for sensitive data encryption and transaction integrity.

Barclaycard in the UK, the first country to roll-out EMV smart cards, in co-operation with Europay International, implemented and piloted the Smart Card Payment Protocol – SCPP – in 1998. However, plans for implementation of additional SCPP pilots are not known.

Also, electronic purses compliant to the Common Electronic Purse Specifications – CEPS, initially conceived for the physical marketplace, use PKC for mutual card-merchant authentication.[10]

The Ducato project, the first CEPS pilot that aimed to validate the CEPS technology and test international interoperability in the physical market place, was successfully completed in December 2001. The first pilot for the use of CEPS purses in e-commerce was announced as part of the BALCARD[11] project, which started in October 2001.

It is interesting to note that both EMV cards support DDA – Dynamic Data Authentication - and CEPS cards require asymmetric cryptographic capability on the smart card, which could be leveraged for other non-payment authentication and digital signature functions based on PKC, such as online banking.

EMV and CEPS Certification Authorities have a hierarchical model and are managed by the schemes (Visa and Europay/MasterCard manage the root CA) and by the banks.

Although these solutions may play a significant role in the future, the slow deployment of smart cards and the limited availability of smart card readers decrease their role as a short term solution for Internet payments.

5.1.5 Use of PKI by Payment Service Providers (PSP)

New models have appeared which build a direct trust chain between consumers and merchants. These banking and non-banking initiatives aim to strengthen consumer and merchant authentication by establishing the Payment Service Provider as trusted third party, establishing bilateral relationships with consumers and merchants. This model allows secure but simpler authentication techniques (such as PIN or passwords, e-mails, etc). In addition, it avoids transmitting the consumer payment data to the merchant.

[10] Merchant authentication is implemented through the authentication of the PSAM (Purchase Secure Application Module).
[11] Project co-ordinator: Mellon s.a.

To our knowledge, three PSPs are using PKC for authentication – all at pilot stage and with limited national scope.[12] Jalda uses PKC for consumer authentication and MoverCard and Cartio for both consumer and merchant authentication. Of these three, only MoverCard makes use of smart cards to store secret keys and generate digital signatures. Non-repudiation enforcement is governed by a contractual relationship.

The three PSP's act as Certification Authorities, issuing certificates to the participants. However, Jalda allows the use of certificates issued by other entities.

5.2 USE OF PKI FOR MOBILE PAYMENTS

A number of mobile payment pilots have been announced by telecom providers and the banking schemes, with a variety of architectures (dual chip[13], dual slot[14], single chip card[15]) and security approaches to be tested. Some of them, described in Table 3 overleaf, make use of PKI for consumer authentication and payment order signature.

As regards using PKI for authentication and signature, mobile infrastructure offers the possibility of using the available SIM (or a second chip) to securely store the private key and generate the digital signature, thus making it possible to legally bind the consumer to the purchase order.

In addition, the use of digital signatures allows non-bank players to provide mobile payment services, as do France Telecom Mobiles, taking advantage of their relationship with consumers and their micro-billing capabilities.

We have found a significant number of PKI pilots, in line with market forecasts predicting a major growth of the PKI market in the mobile sector (Datamonitor, May 2001). Despite the lack of standardisation in wireless PKI, these initiatives could be an indication of the importance of security for the future growth of mobile services, and the potential adequacy of PKI based security solutions to this environment, as pointed out earlier.

[12] Jalda national implementations are in Sweden, UK, Italy, Netherlands and Finland; MoverCard implementation is in Italy; and Cartio in the Netherlands. See ePSO-Inventory (http://epso.jrc.es/paysys.html)
[13] Nordea and Visa International EMPS project, Mobey Forum's Preferred Payment Architecture
[14] France Telecom Mobiles with Cartes Bancaires, Cyber-COMM, FINREAD project
[15] banxafe (Banksys), Payitmobile (GZS), Mobitrust (France Telecom Mobiles)

Table 3: PKI initiatives in the mobile payment sector

Actors	Service	Announced	Pilot plan	Solution
Nordea, Visa International, Nokia	EMPS – Electronic Mobile Payment Services	May 1999	Sep 2001 (started)	Dual chip following 3D-SSL model
Sonera SmartTrust, Europay International	Mobile payment	Jan 2001		Wireless PKI integrated into 3D-SET. Uses a single chip card and SMS. *Sonera Smart Trust's solution aims at complying with local legislation for digital signatures.*
France Télécom Mobiles, CertPlus	Mobitrust	Mar 2001	Summer 2001, 1Q2002	One chip card
Mobey Forum[16]	'The Preferred Payment Architecture'	Jun 2001		The solution allows the issuer to choose the end user authentication method, though the preferred solution is a wireless PKI based on a dual chip phone.
Nordea, UBS	Mobile payment	Sep 2001	Sep 2001 (pilot)	Dual chip phone, in line with the architecture promoted by Mobey Forum.
RadioLinja, Visa Finland (Luottokunta)	Mobile payment	Jul 2001	4Q2001	One chip card

These solutions are mostly in progress or at pre-pilot stage. Their results and the degree of consumer adoption will tell whether this is *'the'* or *'one of the'* possible ways forward to building a secure platform for user authentication and signature in Internet commerce.

5.3 USE OF PKI IN OTHER APPLICATIONS AND MARKET SEGMENTS

5.3.1 Use of PKI in B2C non-payment applications

If we look beyond payments in the retail sector, we see that there is still very limited use of PKI techniques in the B2C market. Indeed, while financial institutions use SSL to secure the transmission of PIN numbers and other confidential account data, only some institutions have started using PKC, PKI or digital signatures to secure online services to their individual customers, as shown in Table 4:

[16] Forum constituted by financial institutions and mobile handset manufacturers to encourage the use of mobile technology in financial services (www.mobeyforum.org)

Table 4: Use of PKI in B2C non-payment applications

Country	Organisation	Services
Ireland	Ulster Bank	Uses PKI since Oct 1999 for securing Internet online banking.
Finland	Oko Bank group Sampo-Fennia insurance group	Oko Bank, uses the FINEID (national Electronic ID) to provide access to Internet banking. Sampo-Fennia, uses the FINEID and digital signatures to provide online services to consumers.
Germany	Sparkassen-Finanzgruppe	Announced the roll out of PKI on May and July 2001 (www.financialnetalert.com). 600 Savings banks will act as CA and issue 20 million smart cards, which will contain digital certificates and be compliant with digital signature law, for authentication and digital signature of e-banking transactions. The roll out of these smart cards will however be graduate following market demand.
Netherlands	PostBank and Telfort GSM operator	Announced the launch of a mobile banking service in summer 2001 to 500.000 potential customers. There are plans to expand to mobile payments.

5.3.2 Use of PKI in B2B applications

Financial and non-financial companies have been conducting secure information exchange through EDI and using authentication mechanisms for many years. PKI, with its new security and key management mechanisms, has been implemented in the B2B market sector mainly for e-banking applications. Relevant initiatives, both international (Identrus, GTA – Global Trust Authority, SWIFT TrustAct, and ELEANOR payment initiation) and national (Isabel in Belgium, ECPS – European Council of Purchasing and Supply – in the Netherlands, eGiro in Norway), should be mentioned.

Other PKI-based applications used in B2B commerce are time stamping, document notarisation, digital proof of receipt, secure file transfer, mail and web forms.

5.3.3 Use of PKI in the public sector

In most European countries there are on-going e-government initiatives (see Appendix D) which are considering or already making use of PKI for access and digital signatures. These initiatives pursue the following benefits:

1. time savings for information processing inside the government bodies and reduced response time to citizens and businesses;

2. cost savings as a consequence of decreased transaction time and cost, increased accuracy and productivity, reduced paper-based maintenance and operating costs, better and more trusted ways of allowing users to pay for services provided;
3. enhanced service to inside users, to the public and other entities;
4. improved quality and integrity of data, compared to paper-based systems.

A rapid development of e-government can be expected in the next few years, fostered by the eEurope initiative and action plan (June 2000, March 2001) among others. The work programme includes efforts to address mutual recognition and interoperability for the provision of trans-border and pan-European applications.[17] The development of PKI and digital signatures in this sector is also expected to grow following the Ministerial Declaration (Nov 2001) on the agreement to support the large-scale use of electronic signatures.

A high level analysis of market players indicates that the financial institutions, governments, telcos and postal services are the leaders in the implementation of PKI services for the consumer market.[18]

Finally, apart from pilot experiences, very limited public-private co-operation is observed (see Appendix E). What little there is generally takes the form of telcos providing PKI Certification Authority services to governments.

Although the implementation of PKI systems for digital signatures, e-ID, or e-government services is only in the initial stages, it has already come up against the following barriers:

- Complexity and costs of the solutions.[19]
- Lack of consumer incentives (e-applications, convenience) vs. costs (card, reader, software)
- Lack of standards, in particular for the interoperability of certificates and signed envelopes, the cross-checking of certificates issued by a third party CA, the usage of certificates by applications, the certificate handling by directories, and time stamping. In the absence of standards, some countries in the process of implementing PKI for

[17] Among the e-government initiatives, it is worth mentioning FINEID in Finland as the first world-wide Electronic ID and digital signatures (PKI-based) project rolled-out on Dec 1999.

[18] In most of the European countries, telcos are providing CA services either on their own (Austria, Belgium, Italy, Netherlands, UK, etc), in alliance with banks (France, Germany, Spain) or in alliance with the postal services (Norway). In some countries, postal service organisations are also providing CA services on their own (France, Ireland, Netherlands, Sweden, UK).

[19] According to Gartner Group, about 80% of PKI pilots have been abandoned by companies because PKI is difficult to install and expensive to use. The complexity of establishing trust models for authentication, the

digital signatures have developed their own specifications[20], with may lead to interoperability problems in the future.

- The legal and procedural regulation aspects of building mutual trust worthiness recognition across CAs and across countries and related jurisdictions, that is, mutual recognition of policies, contractual agreements and legal frameworks (on digital signatures and contractual liabilities).
- Difficulties in building technical interoperability across different CAs, in particular, at application level, in the use of cryptographic techniques, attribute certificates, smart card technologies and registration schemes. National, European and global fora and working groups are intensively debating these issues, developing potential interoperability models[21], and carrying out pilots to achieve both technical and legal interoperability (see Appendix F).

Additional problems in relation to large-scale implementation are predicted (Spafford, 2002). These are, for example, the potential threat to consumer privacy as individuals' information is made available within the certificates, the complexities of key revocation requiring the management of large and highly available revocation lists and the distribution of liabilities between the certification authorities and the businesses using certificates in case of abuse.

5.4 CONCLUSIONS

While PKC is broadly used on the Internet to provide data confidentiality and integrity (SSL), PKI is still in its infancy with regards to authentication and non-repudiation both in the B2C e-commerce segment and e-government G2C sector.

Banks' attempts to use PKI for authentication and non-repudiation in B2C Internet payments have failed to gain extensive adoption and these actors have consequently proposed different non-PKI based solutions. The diversity of approaches throws market adoption and interoperability into question.

Other Payment Service Providers are also generally using non-PKI based security techniques for authentication. However, we also observe that some payment service

difficulty in integrating with internal applications and the intricacy of managing certificates being the major reasons (http://www.informationweek.com/776/document2.htm)

[20] E.g. SEIS Swedish standard adopted also by Norway.

[21] Cross-certification, Bridge CA, cross-recognition, Certificate Trust List, Accreditation Certificate, Strict hierarchy and Delegated path discovery and validation.

providers are starting to use PKI. In parallel, PKI is emerging for mobile payments, online financial services and e-government applications.

Both private and public initiatives have encountered common barriers for the implementation of PKI in the initial implementation stages (lack of consumer incentives for adoption vs. costs and effort, costs and complexity of the solutions, technical interoperability among vendors). E-government initiatives, however, are facing particular legal, procedural and technical interoperability problems in their efforts to achieve mutual recognition across CAs and across countries.

6 CONCERNS RELATED TO THE USE OF PKI FOR INTERNET PAYMENTS

Comparing the potential use of PKI and digital signatures with their actual use for payments, we would like to present some concerns, which challenge the widespread assumption that common focus of PKC, PKI, digital signatures and secure Internet payments will lead to a secure and trustworthy environment for e-commerce.

6.1 PKI AND DIGITAL SIGNTURES MAY NOT BE AN ADEQUATE SOLUTION

Our analysis leads us to the concern that PKI and digital signatures may not be an adequate solution for authentication and non-repudiation for Internet payments. A number of inherent characteristics of PKI create implementation barriers which will be difficult, or require a long time to overcome, such as:

- the cost of PKI-based solutions,
- the existence of competing cheaper and simpler solutions,
- the difficulties in building technical, procedural and legal interoperability of implemented PKI solutions,
- the need to adapt the business model, in order to achieve a greater balance between benefits, costs and liabilities.

However, looking at the potential of PKI, one could also argue that, among the elements that have hindered its deployment, some could be considered as temporary or due to a series of avoidable implementation weaknesses, rather than to PKI itself. Some of these include:

- the lack of smart card infrastructure, which could change by 2005 with EMV planned migration,
- the lack of smart card readers, which could also change by 2005 as PC manufacturers deliver PCs with smart card readers as standard configuration, as iTV Set Top Boxes are delivered with a standard second smart card reader (EMV compliant), or as mobile devices are adopted as authentication devices,
- the lack of a legal framework and solutions for digital signatures, which could change with the recent EC Directive deadline for its adoption into national law and with the potential deployment of PKI solutions for digital signatures and e-government services.

6.2 THERE MAY BE LOW PROBABILITY THAT BANKS AND GOVERNMENTS CO-OPERATE

Following the analysis of the major challenges faced by private and public actors in the implementation of PKI-based solutions, closer co-operation between banks and governments in the definition and implementation of PKI and digital signatures as a possible way through is considered. The potential benefits in strengthening this co-operation and the major challenges are analysed. Underlying related questions are: should payment applications use legally recognised digital signatures? Should banking authentication be the same as government authentication? Is co-operation necessary to ensure consumer adoption? Is co-operation necessary for a cost-effective implementation of PKI?

Our analysis leads us to the concern that, in spite of potential synergies, the different interests and requirements of banks and governments, and the potential challenges of co-operation, it could be unlikely that banks and governments co-operate more in this area, as the benefits would not offset the difficulties.

Different objectives and requirements

Market analysis and development show that the two pioneer sectors in authentication services are governments and financial institutions, and that both may take a role as trust leaders. However, the case for PKI for each is different:

- The benefits of using PKI for governments include increased internal government efficiency as well as improved services to other government bodies, businesses and citizens. Financial institutions, on the other hand, aim to enhance their e-banking solutions for their corporate and, to a lesser degree, individual customers.
- Banks may make use of their own PKI solutions, governed by contracts and independent of the legal, technical and policy framework of legally recognised digital signatures and interoperability requirements governments will need to consider.
- Governments, while needing interoperability among the different governmental bodies (central and local administration entities), have a smaller priority for building interoperability with other countries, while banks, in order to offer e-payment services through open networks, need to build cross-country global interoperable solutions.
- Trust, data protection and anonymity requirements of the citizen dealing with governments may differ (depending on culture) from the requirements of the consumer who transacts remotely with an unknown merchant.

- The definition (and required registration procedures) of a digital ID for governments or for concluding a commercial transaction may be significantly different.

Potential synergies

Nevertheless, potential synergies of co-operation have been identified, namely:

- Governments' plans include the implementation of e-government services both towards citizens and businesses, which allow for payments in both directions (e.g. tax payment and refund, payment of family allowance, e-procurement).
- Governments' role in promoting the deployment of e-commerce infrastructure could be leveraged. For example, government initiatives on e-procurement and establishing compulsory use of a particular infrastructure (e.g. smart cards) may foster e-commerce development, if interoperability exists.
- Co-operation in building PKI solutions could contribute to the development of a competitive PKI services market, and sharing of infrastructure costs (CAs, smart cards, readers) could accelerate the deployment of the infrastructure.
- Banks have a number of capabilities that could be leveraged for the deployment of PKI - e.g., wide branch networks and knowledge of their customers, long service in the trust business, experience of mass smart card issue, security and secure infrastructures and risk management. The opportunity to provide some of these services to other non-banking organisations, such as governments, may develop economies of scale and accelerate the development of the PKI services market.
- Co-operation between banks and governments could support a consistent user experience, accelerating consumer acceptance and increasing consumer trust.

Potential challenges to co-operation

Some of the co-operation challenges identified are:

- Governments' decision process can have a centralised top-down approach, while the banks, working from the bottom-up, need to organise co-operation in order to agree on common banking requirements and global interoperable specifications.
- Strong private/public co-operation may increase risks in relation to data protection and consumer/citizen privacy, and create user concerns of a 'big-brother' nature.
- The need to manage a multiplicity of Digital Identity concepts (including use of pseudonyms) to replicate physical situations and to enhance data privacy is a major challenge.
- Finding a co-operation model that would allow an open and competitive PKI services market to be built.

6.3 THE LACK OF CONSUMER ADOPTION COULD REMAIN A MAJOR BARRIER

Among the issues arising when applying PKI and digital signatures for secure Internet payments, the barriers for consumer adoption are a major concern. Today's implementations of PKI for consumer authentication and non-repudiation (that is, security measures that would benefit merchants) impose costs and burdens that are not offset by the consumer incentives. Moreover, feasibility questions arise regarding the application of the non-repudiation concept and the allocation of consumer liability in case of fraud.

Our analysis leads us to the concern that, unless significant numbers of measures are taken both to increase consumer incentives and protection and to reduce burdens, consumer adoption could remain a major barrier to the implementation of PKI for authentication and non-repudiation in Internet payments.

Consumer adoption

There are different reasons why users may hesitate to adopt PKI-based solutions:

- there may be a lack of technical competency and understanding of the technology and of the specific procedures (generate key pair, request a certificate, carry private key),
- procedures may be too cumbersome (register, provide Identification proofs),
- implications and consequences may not be accepted (liability enforcement or loss of cancellation rights),
- and last, but not least, costs play a significant role (if smart cards or biometrics are used, the consumer may have to support the costs of tokens, readers and related software).

So far, the benefits provided by PKI implementation for individual consumers or citizens (SET, Cyber-COMM, FINEID) have proved insufficient for consumer adoption. [22]

Could one state that in the current model used for the implementation of secure solutions, there is a lack of balance between benefits (mostly for the merchant) and costs and effort required on the side of the consumer?

[22] This situation may be improved in the future with the use of mobile phones, however, the solutions and their cost distribution models are not very mature yet.

Non-repudiation

A number of difficulties complicate the enforcement of non-repudiation by digital signatures and the allocation of consumer liability in case of fraud:

- Under current distance selling credit card (not present) rules, consumers have the right or freedom to cancel a transaction, without having to give a particular reason. Where digital signatures are used for payment to reduce non-repudiation risk, consumers will loose the freedom to cancel and may be reluctant to adopt their use.
- Where digital goods are purchased and where non-repudiation enforcement applies, how can the consumer demonstrate a failure in service delivery (in the case of malfunction, merchant fraud or other party fraud)? How to create digital evidence is a problem that remains unresolved.
- There are difficulties in ensuring that the right person has accessed the private key associated with the digital signature being used, in particular when private keys are stored on web servers or server wallets. A breach in security may occur because of the end user's failure to take reasonable steps to safeguard access to a private key. It may also occur because the processes, software and/or hardware used to store the private key and to generate the digital signature have not been made reasonably secure or user-friendly (Whitten, 1999).

  The security strength of the overall PKI is limited by the security strength of its weakest element. Even where private keys are stored on smart cards there are concerns about the inherent weakness of password based security, and also about the vulnerability of many smart card based digital signature solutions available in the market to Trojan horse type of attacks, as recent laboratory tests have demonstrated. (Spalka, Cremers and Langweg , 2001).
- There are no clear standards as yet for what steps users can reasonably be expected to take to keep private keys secure, or how users should be alerted to possible different functions that may be assigned to the use of a digital signature certificate.

APPENDIX A: ABBREVIATIONS USED

B2B	Business To Business e-commerce market segment
B2C	Business To Consumer e-commerce market segment
CA	Certification Authority
CEPS	Common Electronic Purse Specifications
CVC/CVV	Card Validation Code / Card Validation Value
EC	European Commission
EDI	Electronic Data Interchange
EESSI	European Electronic Signature Standardisation Initiative
EMV	Europay, MasterCard and VISA integrated circuit card specifications for payment systems
G2C	Government To Consumer sector
G2B	Government To Business sector
GBDe	Global Business Dialogue on electronic commerce
iTV	Interactive TV
PDA	Personal Digital Assistant (hand held device)
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PSP	Payment Service Provider
RA	Registration Authority
SET	Secure Electronic Transaction payment protocol defined by VISA and MasterCard
SSL	Secure Socket Layer
OECD	Organisation for Economic Co-operation and Development

APPENDIX B: INTRODUCTION TO PKI

BASIC CONCEPTS

Symmetric (or secret key) cryptography for encryption is based on the idea of a shared secret. Two parties that want to communicate securely first agree in advance on a "secret key" that allows each party to both encrypt and decrypt messages, making use of the same agreed algorithm, that can be publicly known.

Drawbacks of symmetric cryptography are mainly related to the key management and key distribution aspects:

- exchanging secret keys is unwieldy in large networks,
- the sharing of secret keys requires both senders and recipients to trust, and therefore, be familiar with every person they communicate with securely,
- it requires a secure channel to distribute the "secret keys" in a first place.

Asymmetric (or public/private key) cryptography is based on the idea of a matched cryptographic key pair, split into two sub-keys: the private and the public. A participant willing to receive encrypted communications will first generate a key pair, keep the private key as a secret and publish the public key to all parties that would like to encrypt data for him. Encryption of data only requires access to the public key and decryption of data to the private key. Also, the same participant can encrypt the data with its private key, and the receivers can decrypt it using the public key.

This cryptography resolves the problem of the key management and distribution.

Drawbacks of public key cryptography are related to the computational resources required, which may make it impractical for encrypting/decrypting large amounts of data.

Hybrid approach is a combination of asymmetric cryptography to resolve the key management and distribution problem, and traditional symmetric cryptography to encrypt/decrypt bulk data. This is used today by systems like the SSL protocol to secure web transactions, as well as by secure e-mail schemes such as S/MIME, that are built into products like Netscape Communicator and Microsoft Internet Explorer.

Digital signatures combine data hashing with public-key encryption. A cryptographically secure hash function creates a message digest, which is in turn encrypted using the private key of the sender. The original message, together with the encrypted digest, constitute a digitally signed message. On receipt, the receiver decrypts the digest using the sender's

public key and compares it with the result of an independent computation of the message digest using the same hashing algorithm. If the two values are the same, the message is correct. Any modification of the message through the transmission would lead to a different digest value. Digital signatures do not imply the encryption of the message itself.

Digital certificate is an electronic file that uniquely identifies an entity (and enables secure and confidential communications). A digital certificate binds a public key to an entity in a 'trusted third party' or 'certification authority (CA)' cryptographic system. It contains the public key, identification information of the key holder, information of the key certificate issuer and all the data is bound by making use of a signature with the CA private key.

When one party wants to identify itself, it sends its digital certificate to the other party (or the other party can consult the certificate in a Certificate Repository). The other party can, in turn, validate the digital signature of the certificate by making use of the CA public key, validate the identification of the CA and validate the identification of the sender by making use of the information provided by the sender's certificate.

After this authentication process is achieved, the public key of the sender can be used to securely exchange encrypted information with him, and or to verify digital signatures.

Different levels/classes of certificates can exist for different purposes, linked to the degree of reliance that can be placed on a certificate. This mostly depends on registration procedures.

Certificates follow the X509 standard, version 3. In this standard, not only an identity is specified, but also policies that govern the certificate's use, for example to limits its use for transactions below a specified amount, or within a specified geographical region, or for a specified application.

Attribute Certificate, is a certificate which holds attribute information and makes a pair with the certificate holding identity information. Both these certificates are related to the same entity. Attribute certificates can have a shorter life span than their counterpart identity certificates. The update of entity attributes can be achieved by re-issuing the attribute certificate without the need to re-issue identity certificates, and placing the old ones in the CRL.

Certificate policy (CP), is the set of policy requirements (technical, business and legal) governing the creation and use of PK certificates. It indicates the applicability of a certificate to a particular community and/or class of application. It also defines the parties (Subscriber – e.g. consumer, Relying Party – e.g. Merchant and CA) and their relationships and obligations to each other. Policy identification information is also contained in a certificate.

Certificate Practice Statement (CPS) is the statement of practices that a CA will use to issue and manage certificates. It enables relying parties and subscribers to assess the level of trust they may have in the CA and the certificates it issues. A CA's CPS may support different CPs and multiple CA's CPS may support the same CP.

PKI Disclosure Statement (PDS) provides more concise and user-friendly information regarding the "policies and practices employed by a CA/PKI". It may become the accepted basis for conveying legal notice and disclosure to end-users.

Certificate Repository contains a public list of certificates where the relying party can find the subscriber's certificate. However, certificates can also be exchanged between the two parties, for example via e-mail.

Certificate Revocation List (CRL) is a list of certificates that are invalid before their validity dates expires. Certificates are listed here when there has been a change in the identification attributes of the entity, role, privileges, etc or when the certificate holder fails to meet its obligation under the CP, the CPS or any regulatory or legal requirement, or when there has been a security breach. When a certificate is revoked, it is removed from the Certificate Repository and registered on the CRL.

Certification Authority issues, creates and signs certificates and may play a role in their distribution, by the management of the certificate repository. Accreditation of a CA refers to the process of evaluating and certifying the trustworthiness of the authentication and certification services.

Registration Authority is the organisation in charge of verifying the validity of the identification data provided by the key holder, when requesting a certificate.

Applications make use of PKI. PKI is an infrastructure, like a highway. By itself it does little. It starts to be useful when application programs employ the certificates and services that it supplies.

PKI Infrastructure (the "I" of the PKI). In order to provide the authentication, confidentiality, integrity and non-repudiation services a whole infrastructure is required. This consists of cryptography hardware and software technological components, policies governing the use of the PKI, risk management controls, applications that make use of these features, operational rules, organisational practices, contractual agreements among the subscriber and the CA, and the merchant and the CA, data privacy agreements, and legal framework.

ROLES / SERVICES

The *subscriber* is the entity that is registered at the *Registration Authority,* requests a public key certificate to the *Certification Authority* to allow authentication by other parties and, makes use of the secret key to encrypt data and digitally sign data. In the payment context, this would be done by the *consumer*.

The *relying party* is the entity that, trusting the *Certification Authority,* makes use of the *Certificate Repository* managed by the *Certification Authority* to obtain the subscriber's public key certificate and uses the *Certification Authority* public key to validate the certificate. After that, the relying party will verify the documents, digitally signed by the subscriber party using the public key, and will make use of the signature to conclude a binding function (payment, contract, etc). In the e-commerce context, the *relying party* is generally *the merchant.*

The *Certification Authority,* therefore, acts as an intermediary organisation that knows both transacting partners and establishes trust between the subscriber and the relying party, who do not know each other. It guarantees that keys used by the subscriber belong to the entity that the relying party wishes to transact with.

The Certification Authority signs and distributes the public keys and certificates. For that it uses Certificate Directory services and key and certificate revocation services.

In relation to legally binding digital signatures, the CA can also provide Trusted timestamp (to register the date and time when a time-stamp was generated for a message) and notary (to substantiate the validity of digital documents and authors of transactions) services.

MOBILE OR WIRELESS PKI

The same PKI concepts apply to the wireless environment. A PKI is considered mobile or wireless PKI when at least the front-end devices employed by end-users to communicate with other parties are wireless. In other words, wireless PKI is not necessarily completely wireless, it only seems wireless to the user.

Despite their limited CPU, memory, power consumption, and display resources, wireless devices must, in principle, be able to generate and register keys, manage end-user mobile identities, encrypt/decrypt messages, create and sign data, and receive, verify, store and send certificates and digitally signed data. However, in many cases wireless devices are not able to perform all these functions, and a network agent is required to perform some of the functions outside the mobile equipment. This brings a new party into the implementation architecture, which also requires standardisation (Radicchio).

APPENDIX C: SELECTION OF PKI CERTIFICATION AUTHORITIES

CA	Owners	Services	Geographical Scope	Users
Verisign VTN www.verisign.com	Verisign (NASDAQ)	- Internet based certificate issuance and revocation to enable web sites - Insurance and warranty	Global	Web site owners
Global Trust Authority www.gta.multicert.org	Financial Institutions (co-operative)	- Root key CA (Interpay) - Issuer & revocation of MTA certificates - Arbitration Liability risk model	BE, FR, IT, PO, Spain, The Neth	B2B? Master Trust Authorities
Identrus www.identrus.com	Financial Institutions	- Issue certificates - Dispute handling - Warranties - Business & Op rules	Global	B2B Banks (Dec 2000) SWIFT
GlobalSign www.globalsign.net	Vodafone, Ubizen, ING-Barings,Brufico m, GIMV, Technicom, KBC Bank	- Certificates issuing - CA root key signing for cross-certification	Austria, Bel, Lux, France, Germany, UK Italy, Greece	Vodafone UK (mobile pilot announced 04/01)
SET www.setco.org	SETCO (VISA, MasterCard) & VISA CA & EPI/MCI CA	- Root key CA mgt - Generate SET Brand CA certificate - Manage Certificate revocation list	Global	Financial Institutions
EMV www.emvco.org	EPI/MCI CA and VISA CA	- CA Root Key mgt - Issuance of certificates	Global	Financial Institutions
CEPS www.cepsco.org	EPI CA and VISA CA		Global	Financial Institutions
UniCERT www.baltimore.com/unicert	Baltimore (NASDAQ, LONDON)	- PKI CA & RA	Global	Financial Institutions, Governments
ChamberSIgn www.eurochambres.be/chambersign	Chambers of Commerce	- Root CA	Austria, Bel, France, Ger, Ita, Lux, Neth, Spa, Swe, UK	Businesses
Digital Signature Trust – DST www.digsigtrust.com		CA services TrustID Certificates (American Bankers Association ecom) ACES Certificates (US General Services Administration)	US	US consumers, Web site owners, business, government agencies (ACES only)
WiseKey www.wisekey.com	*Swiss financial and Chamber of Commerce org*	*Stopped operations as of end July 2001 due to lack of demand*	*Global*	*World Trade Center, ?*

APPENDIX D: SELECTION OF EU E-GOVERNMENT PROJECTS

Country	Project	Status
EU		
Austria	Citizen Card	
Belgium	Federal Government e-Government: FEDICT Id card	
Finland	FINEID (electronic Id and digital signatures) for e-government administration, education, tax services, social insurance and healthcare services. First EID project in the world. Slower development than expected due to the lack of services relying on the FINEID card and PKI, both on the public and private sector, cost of the equipment (card costs 36$, the smart card reader costs 15$ and the software 16$ for utilising the reader). By October 2000, two banks and one insurance company have launched a FINEID based authentication and digital signature for their web services. Wireless EID announced in January 2000 by Sonera Smart Trust and Finnish Population Register Center.	Deployment Dec 1999 (voluntary) In July 2001: 10000 cards requested (out of 5 million citizens)
France	TéléTVA – VAT declaration GIP-CPS – Authentication and digital signature in the health environment AdeP - multi-usage citizen card	Started May 2001 Production, 350.000 cards Oct 2001 Target 1 million cards by 2006 2001: Prototype test 2001-2002 : Large scale deployment
Germany	SPHINX, e-mail encryption and signature in government (www.bsi.bund.de/aufgaben/projekte/sphinx/index.htm) Media@Comm Federal Government announces (Jan 2002) introduction of electronic signatures for its employees	 Deployment planned 2002-2005
Italy	Italian Government Electronic Identity card (with Baltimore) for electronic identification, authentication, network transactions' communication security and digital signatures features to be used for communication with the citizen and deliver e-government services (healthcare, voting, social security, transportation and education).	Announced March 15th, 2001. Issuance of 100,000 cards is planned by June 2001, 1 million by 1Q2002 and up to 60 million over the project period.
Netherlands	PKI Overheid: e-voting, information to citizens, tax payment, health care, social benefits	2001-2002: Requirements and pilots. 2003: (Pre-) implementation. 2003-2005: large scale roll-out. Target 20 million cards.
Portugal	National ID card	
Spain	TASS, CERES e-government, in social insurance Generalitat Valenciana to issue digital certificates to citizens and staff to provide authentication, secure communications and non-repudiation for the provision of e-government services (employment, training, electronic transfer of legal documents) GISA, Catalan Government project for public procurement by electronic signing of the whole documentation associated with a work contract Xunta de Galicia, Secure web access by companies Minister of Agriculture, Project Land: Consultation	Since 1999? Announced 18 Jan, 2001 Pilot planned for June 2002 Full deployment: Jan 2003 with target of 5 million cards
Sweden	Education, employment, taxes, social services, vehicle registration services. Swedish SEIS electronic ID, PKI and smart card based project – Merita Nord Banken issued 35K cards (end 1998) SEIS compliant to home banking customers	Gov. using PKI since 96. Tax pilot underway with Post certificates. 50.000 Post certificates issued end 2001. Target for 2002 is 150.000 cards and 6 million for full deployment
UK	Could Cover Initiative	

APPENDIX E: SELECTION OF PUBLIC / PRIVATE CO-OPERATION INITIATIVES

Country	Project	Description
EU		
Italy	AIPA (Authority for IT in the Public Administration), Banca d'Italia, Italian Certification Authorities	In support of an effective spread of the electronic signatures, a "Working Group for the Certification Authorities' Interoperability" was established by AIPA to understand if and how interoperability among CA's could be established. The WG has produced the 'Interoperability Guidelines' as the result of the definition and operational verification of a set of technology independent interoperability rules. The definition approach has been based on operational and practical solutions to the identified problems, on the market availability of the tools needed to realise them, on simplicity and applicability to all CA's. Consistency with on-going standardisation processes in the field of electronic signatures has also been taken into account.
UK	Barclays Endorse	Smart card digital signature service, launched in June 1998. The Government was first to make use of this service enabling the newly self-employed to register their tax status across Internet. Service is open to all, neither the acceptor nor the cardholder need to be existing customers of Barclays Bank. Different levels of security and liability are provided. Looking for new commercial opportunities within the private sector as well as continuing to support Government's applications in the public sector.
UK	Vodafone UK, Government - Department of Trade & Industry, Radio Communications Agency (RA), Smart Trust	Start of a technology trial on July 2001. 50 staff complete and sign travel or subsistence forms in Internet and sign the complete form by using their mobile handset. A hash of the form and completed information is sent to the user via SMS, who signs this information by entering a signature PIN on his mobile. Project is a proof of concept, focusing on technology.
Norway	Telenor and Ergo Group (previously Posten SDS)	Have built a CA that provides services to the government
Sweden	Swedish Post and Telia	Provide certificate for internal government services. Contract negotiations undergoing for banks to issue citizen certificates.
Fi, Fr, Ger, Irl, Isr, It, Spa	EEPOCH (eEurope SC)	Multi-application card with EID, digital signature and financial applications (timing: under definition in the eEurope Smart Card initiative)

Country	Project	Description
Outside Europe		
Japan	Co-operation-platform	Pilot planned for a contact-less multi-application smart card based cyberspace passport, an electronic Id to check the cardholders' citizenship, issued by the government on request when people want to receive e-government services in the cyberspace. May also record services that the holder receives at his request (public and private applications) and could also support electronic signature (PKI). 1 to 3 million cards are planned by the end of 2001, 10-50 million people are expected to have cards from Aug 2003.
Malaysia	Co-operation smart card platform	A government multi-purpose card (24 July 2001). The GMPC, the Government Multi-Purpose Card will replace the Malaysian national identity card and driving licence. Will also contain passport information, national health application and non-government applications such as e-purse, ATM cash withdrawal application and digital signature application based on the PKI. 600,000 cards are planned by end of 2001, rising to 19 million by the end of 2008.

APPENDIX F: PKI INTEROPERABILITY INITIATIVES

Some of the interoperability initiatives	
International initiatives	CEN-ISSS EESSI – European Electronic Signature Standardisation Initiative eEurope, eEurope SmartCards and related initiatives: - TB1 Public Identity - TB2 Identification and Authentication - TB4 Generalized card reader - TB10 e-Government - TB12 Advanced Electronic Signature - Global Interoperability Framework, in particular for Identification, Authentication and electronic Signatures with Smart Cards - Co-operation with Smart-IS and CEN-ISSS WS/e-Sign Area K - EEPOCH field trial IDA – Interchange of Data between Administrations EEMA – The European Forum for Electronic Business ECAF – European Certification Authority Forum PKI Forum PKI World OECD Radicchio m-sign Asia-Pacific Economic Co-operation – APEC Forum EMA – the Electronic Messaging Association Global Business Dialogue on Electronic Commerce
National initiatives	**UK**: CESG Cloud Cover Interoperability Testing **Germany**: Deutsche Telekom-Deutsche Bank-Federal Government and Lan Thüringen, **US**: Federal and DoD Bridge CA Initiatives **Canada**: Government of Canada PKI project **Australia**: Australian Government Gatekeeper Project **Italy** : Interoperability Guidelines defined by AIPA (Authority for IT in the Public Administration), Banca d'Italia and Italian Certification Authorities
Technical interoperability pilots	**EC** funded: ICE-TEL and PKI Challenge projects **European** Bridge CA **US**: PKI Interoperability Testbed **EMA**: Federal Governments of US and Canada
Accreditation interoperability initiatives	**European** EESSI Common Criteria **UK**: British Standard – Code of practice for Information Security management **US**: PAG – The PKI Assessment Guidelines (ABA) RFC 2527: Framework for PKI policy documents AICPA/CICA WebTrust Program for Certification Authorities X9.79 – CA control Objectives (A Bankers A) **Australia** : Gatekeeper

BIBLIOGRAPHY

Adams, Jane
Smart Cards Meet the Future In Finland, CardTech Issue October 2000, (http://www.cardtech.faulknergray.com/oct00.htm)

American Bar Association Information Security Committee
Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, August 1996, (http://www.abanet.org/scitech/ec/isc/dsgfree.html)

American and Canadian Institutes of Chartered Accountants
Web Trust Principles and Criteria for Certification Authorities, February 2000, (http://www.aicpa.org/homepage.html) [Provides a framework to assess the adequacy and effectiveness of the controls employed by CAs]

APEC Telecommunications Working Group, Business Facilitation Steering Group
Electronic Authentication Task Group, Issues relating to the use of Electronic Authentication, March 99, (http://www.apii.or.kr/apecdata/telwg/eaTG/eaTG-2.htm)
E-Commerce in government Issue Paper, draft version for discussion, March 2001 (http://www.apectelwg.org/apecdata/telwg/23tel/bfsg/bfsg_12.htm)

Bensoussan, Alain – Alain Bensoussan Avocats
Electronic signature and evidence. Presentation and proceedings of conference "Cartes 2001", Paris, October 2001.

Berlecon Research
Kassieren im Ecommerce - Eine Analyse relevanter Zahlungssysteme aus Händlersicht (Getting your bills paid in e-commerce). Berlin: Berlecon Research 2001; extracts at http://www.berlecon.de/studien/zahlungssysteme/en/index.html [Study analysing the merchant side of Internet payments. It underlines the role of those payment instruments most heavily used in the traditional MO/TO sector for e-tailers too.]

Böhle, Knud – IPTS JRC European Commission
Electronic Payments 2001 – Food for thought, ePSO-Newsletter No.8, July 2001 (http://epso.jrc.es) [Presents topics on e-money and the EMI directive, loyalty schemes, and the challenges banks and credit card associations face today, as discussed in the Net Profit Finance on e-payments report]

Böhle, Knud and Krueger Malte – IPTS JRC European Commission
Payment Culture Matters – A comparative EU – US perspective on Internet Payments, ePSO project – Background Paper No.8, May 2001 (http://epso.jrc.es)

Boncella Robert J., Computer Information Science Department and School of Busines Washburn University (zzbonc@washburn.edu)
Web security for e-commerce, Communications of the Association for Information Systems, Volume 4, Article 11, November 2000. [Presents an overview of the major categories of the Web site attacks, their effects and possible countermeasures. The focus is the Web security necessary for a reasonable guarantee of secure e-commerce]

Bowman, Louise
Selling Citizens On Smart ID Cards, CardTech May 2000, (http://www.cardtech.faulknergray.com/) [Chip based national Id cards are proceeding slowly, hampered by high costs and political resistance]

Causton, Raymond - Helsinki University of Technology / Department of Electrical and Communications Engineering
FINEID-Project and Need For Privacy, Dec 11, 1999, (http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/fineid/fineid.html), [Discusses the FINEID electronic identity card in the context of retaining privacy in network-based transactions even while using the FINEID-card and PKI for identification]

Clarke, Roger – Department of Computer Science, Australian National University
Public Key Infrastructure Position Statement, May 6th 1998, (http://www.anu.edu.au/people/Roger.Clarke/DV/PKIPosn.html) [Highlights the fundamental tension that exists between the needs of reliability in electronic messaging and the interests of individuals in privacy protection, and suggests a way ahead in the implementation of the PKI architecture].

CommerceNet
EPayments: Is the Credit Card System Failing eCommerce? Is a solution in Sight?, published in the CommerceNet Newsletter "The public Policy Report", Vol.3, No. 5 May 2001, (www.commerce.net)

Computer Security Institute, US
2001 CSI/FBI Computer Crime and Security Survey, Published in the Computer Security Issues and Trends magazine, Vol. VII, No.1, Spring 2001, (www.gocsi.com)

EESSI, European Electronic Signature Standardization Initiative
First Set of Deliverables, April 2001, (http://www.ict.etsi.org/eessi/ddd.doc) [Presents the achievements of the EESSI in the execution of the mandate given by the European Commission to the ICT Standard Board for the delivery of a set of industry specifications that will facilitate a consistent and coherent implementation for validity and cross-recognition of Directive 1999/93/EC on a Community framework]

Signature Creation Process and Environment CWA 14170, Oct 2000, [Specifies the Signature Creation process and environment to create Advanced Electronic Signature with the help of the Secure Signature Creation Device and the Signer's Signature Creation Data using Qualified Certificates].

eEurope Smart Card Charter – Trailblazer 2 on Identification and Authentication
A pre-inventory of smart card based PKI projects within the EU, December 2001

Egger, Florian N. and Abrazhevich, Dennis – Eindhoven University of Technology, The Netherlands
Security & Trust: Taking Care of the Human Factor, ePSO-Newsletter No.9, September 2001 (http://epso.jrc.es) [Puts forward a user-centred perspective of the problem of trust in online payments, derived from the discipline of Human-Computer Interaction (HCI)]

Electronic Commerce Branch Industry Canada
Building Trust and Confidence in Electronic Commerce: A framework for Electronic Authentication in Canada, July 2000, (http://e-com.ic.gc.ca/english/documents/framework.pdf) [Describes electronic authentication and certification services. It identifies the need to provide a co-ordinated approach that a framework be established and that international dimensions must be taken into consideration]

Ellison, C. and Schneier, B.
Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure, Computer Security Journal, v 16, n 1, 2000, pp. 1-7. (http://www.counterpane.com/pki-risks.html)

European Parliament and the Council of the European Union
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Jan 19th 2000

Directive 95/46/EC of the European Parliament and of the Council of 24 Oct 1995 on the protection of individuals with regard to the processing of personal data and on the movement of such data.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts.

Directive 1999/1720/EC of the European Parliament and of the Council of 12 July 1999 adopting a series of actions and measures in order to ensure interoperability of access to trans-European networks for the electronic interchange of data between administrations (IDA).

Directive 97/66/EC of the European Parliament and of the Council of 15 Dec 1999 concerning the processing of personal data and the protection of privacy in the telecommunications network.

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.

European Commission
97/489/EC Commission recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder (for which a directive proposal is expected by end 2001).

Study on the implementation of Recommendation 97/489/EC – Final report 20 March 2001. (http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/study.html).

EEurope 2002, Draft Action Plan prepared by the EC for the European Council in Feira (19-20 June 2000)

EEurope 2002, Impacts and Priorities, A communication to the Spring European Council in Stockholm, 23-24 March 2001

IDA – Interchange of Data between Administrations, Work Programme 2001, Horizontal Actions and Measures, March 2001

Desmond, Paul
PKI Distribution Dilemma, Softwaremag.com, Issue Aug/Sep 2000, (http://www.softwaremag.com/archive/2000aug/PkI.html). [PKI systems are only as secure as the mechanism you use for certificate distribution. And for e-commerce, you should also make sure the buyer will pay]

Fratto, Mike
Certificate Revocation: When Not To Trust, June 26th, 2000 (http://www.networkcomputing.com/1112/1112wsl.html) [Explains managing and applying certificate revocation]

Gartner
Online Fraud Prevention White Paper for the E-Commerce Fraud Prevention Network, 3/14/2001, (www.gartner.com/webletter/amex/index.html)

GBDe - Global Business Dialogue on electronic Commerce
Authentication and Security Issue Group, Policy Paper, Final Draft (v1.2), July 8th 1999 (http://www.nec.co.jp/gbde-auth/previous/july/index2.html)

Goodenough, David – David Goodenough & Associates Limited
A Heretic's view of Certificates, Given to the London Central Branch of the British Computer Society on April 20th, 2000. (http://www.dga.co.uk)

The Government of Iceland's Committee on PKI
Preliminary Study on Requirements and Comparable initiatives in other countries, KPMG, May 2001. (http://brunnur.stjr.is/interpro/fjr/fjr.nsf/Files/KPMG-report/$file/KPMG-report.pdf)
[Describes the security requirements of the Government of Iceland, an overview of e-government activities and PKI approaches in Canada, the Netherlands and Sweden, and provides conclusions and recommended next steps]

ICA (International Council for Information technology in Government Administration)
Trusted Services and PKI, ICA Study Group Report, 2000, [Analyses the approaches being adopted in different countries to the provision of Trusted Services and PKI and their role in enabling the secure electronic delivery of government services to the public].

Infocomm Development Authority of Singapore
Infocomm security Technologies in e-commerce, an Infocomm technology Roadmap Report, March 2001, [Technology roadmap of cryptography, public key infrastructure, smart cards, biometrics and digital rights management]

The Internet Council, sponsored by NACHA – National Clearing House Association
The CARAT Guidelines, Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates, Jan 2000, (http://internetcouncil.nacha.org .)

ILPF - Internet Law and Policy Forum
International Consensus Principles for Electronic Authentication, April 1999, (http://ilpf.org) [These principles are intended to facilitate global electronic commerce based on the creation of predictable legal environment for electronic authentication which protects users and reflects their needs]

The role of Certification Authorities in Consumer Transactions – A report Of the ILPF Working Group On Certification Authority Practices, Draft - April 14, 1997 (http://www.ilpf.org/groups/ca/draft.htm) [Presents a preliminary analysis of certain questions relating to legal issues involved in the service business of certification authorities, particularly those arising in consumer transactions].

ITEA Office Association
Technology Roadmap on Software Intensive Systems, The vision of ITEA (SOFTEC Project), March 2001

Klasen, Dirk
Creating Consumer Confidence: Current Efforts towards International Quality Criteria for E-Commerce, ePSO-Newsletter No.9, September 2001, (http://epso.jrc.es)

Laing, S.G.
Attribute certificates – a new initiative in PKI technology, White Paper, 2001 (http://www.baltimore.com/library/whitepapers/acswp-hm.html)

Lelieveldt, Simon
New payment authentication methods for use on the Internet, ePSO-Newsletter No.8, July 2001 (http://epso.jrc.es). [Describes the three models for authentication over the Internet, which may be adopted by Visa (3D secure), Mastercard (Secure Payment Application) and Maestro, as presented during the recent Second Edinburgh Financial Cryptography Engineering Conference].

Linden, Michael - Kanner, Janne - Kivilompolo, Mika - Tampere University of Technology
FEIDHE (a project), Electronic Identification in Finnish Higher Education, 2001, (http://www.csc.fi/proj/hst)

Moreau, Thierry - Connotech Experts-conseils Inc.
Why Should We Look for Alternatives to the Public Key Infrastructure (PKI) Model? August 1999, (http://www.connotech.com/alttopki.htm)
Thirteen reasons to Say 'No' to Public Key Cryptography, Draft paper, March 1998, (http://www.connotech.com/13reas.htm)

NIST – National Institute of Standards and Technology
Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, NIST Special publication 800-25, October 2000 (http://csrc.nist.gov/publications/nistpubs/800-25/sp800-25.pdf)

Bridge Certification Authorities: Connecting B2B Public Key Infrastructures, 2000 (http://csrc.nist.gov/pki/documents/B2B-article.pdf) [Describes different PKI architectures, difficulties in connecting the architectures, and how the BCA addresses these issues. In addition, the article describes the BCA concept, BCA deployment in the U.S. Federal Government, and how the BCA enables B2B electronic commerce]

OECD – Organisation for Economic Co-operation and Development
Joint OECD-Private Sector Workshop on Electronic Authentication, 2-4 June 1999, Background Paper on Electronic Authentication Technologies and Issues

Cryptography Policy: The Guidelines and the Issues, March 1997

Guidelines for Consumer Protection in the Context of Electronic Commerce, Dec 1999 (http://www.oecd.org)

Office of Consumer Affairs (OCA) of Industry Canada
Principles for Consumer Protection in Electronic Commerce – A Canadian Framework, November 1999, (http://www.cba.ca/Eng/Publications/Ecomm/principlese.pdf)

Ohyama, Nagaaki – Imaging Science and Engineering Laboratory, Tokyo Institute of Technology. Smart Card as a Second Infrastructure in the Information Society, eEurope Smart Cards, March 2001

Parodie
Critique système Cyber-COMM de paiement par Internet (http://www.parodie.com/monetique)

EEMA – The European Forum for Electronic Business
PKI Challenge (http://www.eema.org/pki-challenge/index.asp)
WP2 N003 – Secure Applications for PKI support, January 31st, 2001,
WP2 N004 – Overview of Directory Issues, February 18, 2001 v1.1
WP2 N006 – Suggested Interoperability Testing, April 10th, 2001
Network and Information Security: Proposal for a European Policy Approach, EEMA and ECAF (European Certification Authority Forum) comments, Draft v0.1, August 2001

PKI Forum
PKI Interoperability Framework, March 2001, (http://www.pkiforum.org/pdfs/PKIInteroperabilityFramework.pdf) [Defines interoperability from the perspective of the PKI Forum, and develops a framework that can be used to discuss the many facets of interoperability in an appropriate context using consistent terminology]

CA-CA Interoperability, March 2001, (http://www.pkiforum.org/pdfs/ca-ca_interop.pdf) [Discusses the issues associated with establishing interoperability between otherwise isolated PKI domains, and to provide recommendations for the way forward]

Biometrics, May 2001, (http://www.pkiforum.org/pdfs/biometricsweb.pdf) [Discuss the basics of biometrics technology and its synergistic combination with PKI technology]

PKI Policy White Paper, March 2001, (http://www.pkiforum.org/pdfs/pki_policy.pdf) [Provides general information about PKI policy, the role that policy plays in a PKI and how that policy applies to both traditional and PKI-enabled business environments. It also addresses the documentation required to support a PKI policy, what is specified in a PKI policy, how a PKI policy can be managed, and outlines some high level issues regarding PKI policy].

Radicchio
Wireless PKI: Fundamentals, Wireless PKI: Opportunities, Legislation and PKI Evolution (http://www.radicchio.org)

Romppanen, Minna and Vänttinen, Sanni - Helsinki University of Technology / Telecommunications Software and Multimedia Laboratory
The legislation and its Requirements Regarding FINEID, Feb 24 2000, (http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/legislation/legislation.html) [Discusses Finnish Electronic Identification from legislative point of view. Possibilities and threats are analysed, questions are raised. What is taken care of, what remains to be seen, how will everything turn out?]

Schneider, Bruce – Counterpane Internet Security, Inc
Biometrics: Truths and Fictions, Crypto-Gram newsletter, Issue August 15th, 1998 (http://www.counterpane.com/crypto-gram-9808.html)

SET - Secure Electronic Transaction Specification
Book 1: Business Description, May 31, 1997 (www.setco.org)

Siltanen, Antti – SiltaNet Ltd.
Exploitation of PKI in Finland, Presentation for the Telecom IT Conference Oct 11-12th, 2000 (http://www.eurescom.de/~pub/seminars/past/2000/TelecomIT2000/06Anttisiltanen/tsld001.htm)

Spafford, Gene – Center for Education and Research in Information Assurance and Security (CERIAS)
PKI Forum Exclusive Interview, Feb 2002, (http://pkiforum.com/books/interview_spafford.html) [Discusses his view of, among others, the general security landscape; major challenge in information security; the need for advanced security solutions; security infrastructure; PKI and its difficulty with interoperability; PKI and privacy, organisational control and liability; premature deployment of PKI and its dangers; the need for key back-up and recovery by trusted third parties; the need for security skilled people in academia and in business]

Spalka, Adrian – Cremers, Albin B – Langweg Hanno – Department of Computer Science III, University of Bonn
The Fairy Tale of 'What You See Is What You Sign' – Trojan Horse Attacks on Software for Digital Signatures, June 2001

STAR - Socio-economic Trends Assessment for the digital Revolution
E-payments: Which Systems in Europe for the Coming Years? Issue Report N.13 June 2001, by David Bounie and Livio Vaninetti [Examines the competitivity of a chip associated with the SET payment protocol – CyberCOMM – in opposition to the Secure Socket Layer communication protocol]

Stroborn, Karsten
Online-Umfrage: So will der Kunde im Internet bezahlen. In: IIR: C@shWorld. 5. IIR-Kongress Zahlungssysteme im eBusiness., 6.-8.2.2001. Proceedings. Frankfurt am Main: IIR 2001.
[The survey underlines the role of traditional payment methods even for experienced Internet users and savvy online-shoppers. Results of study online at http://www.iww.uni-karlsruhe.de/IZV4/ (in German)]

Øygarden, Kjartan – University of Oslo / University of East London
Constructing security – The implementation of the SET technology in Norway, 2001 [Uses the Social Construction Of Technology approach to see how the SET implementation was conducted and how the different social groups responded to the introduction of the SET technology in Norway]

Van Hove, Leo – Free University of Brussels, Belgium
The Payment Blues of German Internet Merchants, ePSO-Newsletter No.9, Sept 2001, (http://epso.jrc.es) [Comments a report from Berlecon Research "Kassieren im Ecommerce – eine Analyse relevanter Zahlungssysteme aus Händlersicht"]

Verisign
Building an E-commerce trust Infrastructure, White Paper, 2000, (http://www.verisign.com/)

VISA EU – Virtual VISA
Three domain Model Fact Sheet, August 2000, (http://visaeu.com/virtual_visa/presscentre/factsheets/three_domain_model.html)

Wilberg, Torbjörn – Umeå University of Sweden
PKI and Electronic Identity, Sep 29th, 2000

Winn, Jane K.
The emperor's new clothes: The shocking Truth about Digital Signatures and Internet Commerce, Revised Draft – March 9, 2001 (http://www.smu.edu/~jwinn/shocking-truth.htm)
[Critiques specific set of assumptions about specific application of digital signature technology: that contracts will be formed over the Internet among parties with no prior relationships through reliance on digital signature certificates issued by trusted third parties establish the identify of the parties].

Whitten, A – Tygar, J.D.
Why Johnny can't encrypt: A usability evaluation of PGP 5.0, in the Proceedings of the 8th USENIX Security Symposium, 1999 (http://www.usenix.org/publications/library/proceedings/sec99/full_papers/whitten/whitten_html/index.html)

Additional useful PKI links

- Developments relating to standards and specifications, (www.diffuse.org)
- europa.eu.int/ISPO/ecommerce/initiatives/related.html
- RSA Laboratories, (www.rsasecurity.com)
- Certification Authorities, CA Initiatives and Authentication Products and Services, (www.qmw.ac.uk)
- PKI Forum Resources, (www.pkiforum.org/resources.html)
- The security Portal for Information System Security Professionals (www.infosyssec.com/infosyssec/secpki1.htm)
- Resources on Legal aspects of PKI (Baker & McKenzie), (www.bmck.com/ecommerce/topic-pki.htm)
- The PKI Page list of resources, (www.pki-page.org)
- Crypto-Gram monthly newsletter by Bruce Schneider, (http://www.couterpane.com/crypto-gram.html)
- CommerceNet (www.commerce.net)