

**European Commission - DG INTERNAL MARKET**  
**Unit F/2 - Company Law, Corporate Governance, Financial Crime**

**Communication for the open minded**

**Study on user identification methods in card payments, e-payments and mobile payments**

**Work Package 5: Recommendations**

**November 2007**

**SIEMENS**

**SEALED**  
Trust Services Architects

  
**synovate**  
Censydiam

THE HOUSE OF  
**MARKETING**



  
**time.lex**  
Dumortier - Somers - Graux

  
**security**  
4 B i z

Service contract: ETD/2006/IM/F2/92

# *Table of content*

- 1. Introduction**
- 2. Executive summary**
- 3. Conclusions on user identification methods**
- 4. Identified barriers against development of card payments, e-payments and mobile payments**
- 5. Recommendations to overcome the identified barriers**

## ***Objectives of the study and the work package 5***

The objective of this study is to analyse current and prospective cardholder verification methods on card payments, e-payments and mobile payments. The underlying goal of the study is to encourage the payment industry to provide the highest economically viable level of security for those electronic payments but with sufficient consideration of user-friendliness.

The study includes 5 work packages (WP) which address the following topics:

- **WP1**: Assessment of best and most used identification technologies from a security point of view, including payment industry barriers perception
- **WP2**: Assessment of user friendliness of identification methods, including user barriers perception
- **WP3**: Comparison of findings with previous study on user identification methods realized in 2003
- **WP4**: Regulatory, contractual and commercial barriers assessment of best used identification technologies
- **WP 5**: Recommendations

The objective of this document (WP5) is to provide recommendations on the possible ways to address, from a regulatory perspective, any of the identified barriers to enhancing security in these payment systems and to increasing users' confidence and awareness.

WP5 consists of the analysis and assessment of the information obtained in the other four WP and the formulation of recommendations on the basis thereof. In particular, recommendations for improvements to the European and national legal frameworks are drafted based on the results obtained from WP4, and on the findings of the other WP regarding current and prospective user verification methods.

# ***Table of content***

**1. Introduction**

**2. Executive summary**

**3. Conclusions on user identification methods**

**4. Identified barriers against development of card payments, e-payments and mobile payments**

**5. Recommendations to overcome the identified barriers**

## ***From a security perspective, best authentication methods for cashless payments need to rely on two factors***

Each of the payment methods has been assessed in view of its level of security, vulnerability and fraud resistance and its user perception, in order to define the most used and best user identification and verification techniques from a security level perspective.

Independently of the payment type (card, e- or m-payment), two-factor authentication is the expected minimal level of authentication for cashless payments. This is reflected by the security analysis and moreover re-enforced by the legal and regulatory framework.

Payments Cards are the most used payment tool for cashless transaction. The most frequently employed user authentication method is password (e.g. PIN code) based authentication often combined with a “something you have” as an additional authentication factor.

Reasons for PIN being most used are: ease of use, well understood and established amongst users, and no sufficient fraud directly related to this verification method to create a sense of distrust.



**Best user authentication method in cashless payments relies on something you know (e.g. dedicated payment PIN), supplemented by an additional “something you have” authentication factor, in order to implement two-factor authentication**

# From a user perspective, authentication with PIN code or dynamic password are more trustworthy

It is in line with the best 2 –factor authentication method from a security perspective

User identification method	Monthly plus <sup>(1)</sup> frequency of use	User friendliness	Trust in use
<b>Card payment</b>			
• PIN code			
• Signature			
<b>E-Banking</b>			
• Static password (mostly with 1-factor authentication)			
• Dynamic password (mostly with 2-factor authentication)			
<b>E-Commerce</b>			
• Direct with Merchant (mostly static password with 1 factor)			
• Via Trusted Third Party (mostly static password with 2 factor)			
<b>Mobile payment</b>			



User friendliness should be bypassed to the benefit of trust for e-banking and e-commerce, as the dynamic password authentication method is more secure

(1) at least once a month (daily + weekly + monthly)

**Legend:**



# ***Main barriers against the use of cashless payments in Europe<sup>(1)</sup> stem from user perception and commercial model***

- **User perception barriers:**
  - **Caused by the perceived lack of security based on extraordinary negative experiences reported in the news**
- **Commercial barriers:**
  - **Caused by high cost of some technologies**
  - **Caused by the differences in national legislation**
  - **Affecting mainly the Electronic Payment Instruments technology providers, but also the merchants in a lesser extend**
- **However, legal restrictions and obligations, and contractual restrictions are not considered as important barriers against the development of cashless payments**

(1) The present work package only shows the aggregated European results. But is important to note that important differences may exist between European countries, as described in the other work packages.

# ***Recommendations on the legal framework to overcome identified barriers***

- **Increase information sharing for preventing, reporting and punishing fraud:**
  - **Security related information to consumers**
  - **Notification mechanisms in case of fraud**
  - **Suing and punishing identity thieves, while providing recognition to victims**
- **Continue ensuring data protection in current and emerging payment technologies**
- **No need to reinforce the liability of the user or the merchant for current identification technologies, but well the securitization of transactions**
- **Establish harmonization and certification of identification/authentication technologies**
- **Ensure that registration process is made with due care by the involved parties**
- **Reassess the sharing of liability between involved parties for emerging identification technologies**
  - **As it shall be more difficult for a consumer or an Electronic Payment Instruments provider to repudiate a transaction, less liability should be imposed on the merchant (e.g. with e-ID/digital signature)**
  - **In particular, eID cards can be promoted by:**
    - Increasing cross-border PKI interoperability and mutual recognition
    - Better defining liability and control on the issuance in countries where the banks are not part of the issuing process of eID cards
- **If necessary, make recommendations about the interpretation of the Data protection and Data retention Directives in the Member States concerning the retention of traffic data**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

- User identification methods for card payments
- User identification methods for e-payments
- User identification methods for mobile payments
- Innovative user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

## 5. Recommendations to overcome the identified barriers

## ***From a security perspective, the combination of dynamic card authentication and PIN code is the best authentication method***

**Three alternative identification methods are offered for credit cards:**

- **The provision of the cardholder signature, eventually combined with the ID card**
- **The magnetic-stripe cards with the provision of the PIN code at transaction time**
- **The chip cards with the provision of the PIN code at transaction time (additionally to the card information capture)**

**The 2-factor authentication is the best card holder authentication method, which should combination:**

- **The usage of IC Card technology (i.e. chip card) allowing the dynamic authentication of the card at transaction time**
- **The provision of the card holder PIN code as second authentication factor**

**The adoption of IC card authentication in combination with a PIN as user verification method will also be followed by the SEPA Cards Framework (SCF) for implementation in the European member countries.**

**This framework will define a harmonization of minimum security requirements, which allow for functional interoperability of elements of the processing chain for the different SCF compliant schemes, which will:**

- **Be based on the EMV specifications**
- **Adopt PKI-based authentication of the cards (static or dynamic)**

# ***Users prefer to use a PIN code from both a friendliness and trust perspective***

*It is in line with the best authentication method from a security perspective*

**Two alternative authentication methods of card payments were analyzed:**

## **Handwritten signature**

- **Is mostly used for usual household shopping. It is hardly ever used for withdrawing money.**
- **Is seen as a user friendly (81%) application. It is associated in almost all countries with user friendliness and convenience.**
- **Is not able to gain a lot of trust except when people are also obliged to show their ID card.**
- **But the level of trust is consistently higher for a signature combined with an ID card (74%) compared to a signature alone (47%).**

## **PIN code**

- **Is also used mostly for the household shopping, but opposed to a signature, it is a frequently used authentication method when withdrawing cash.**
- **Is seen as more user friendly (90%) and trustworthy (76%) than a signature.**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

- User identification methods for card payments
- User identification methods for e-payments
  - e-banking
  - e-commerce
- User identification methods for mobile payments
- Innovative user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

## 5. Recommendations to overcome the identified barriers

## ***From a security perspective, 2-factor with a dynamic password is the best authentication method***

**Authentication methods in the e-banking environment towards 2-factor authentication methods with EMV authentication is more and more used.**

**In e-banking solution, the use of a PINPAD reader producing a challenge signature based on the user's bank-card seems to generalise. This observation is EU-wide and was quite expectable since there are norms that uniform such payments schemes.**

**An effective way of authenticating users is to use the EMV smart card as authentication means, which can be currently seen as the best technique for authentication in e-banking.**

**Security of e-banking scheme is strengthened by use of a software (e.g. an applet from the bank). This solution helps to struggle against attacks such as phishing.**

**The use of e-signature in the sense of the EU Directive on e-signature is a real evolution that helps to sustains non-repudiation litigations.**

# ***Users prefer dynamic password from a trust perspective, but not from a friendliness perspective***

*It is in line with the best authentication method from a security perspective*

**Online payments are payments for goods and services via the internet. Payment via the internet is mostly done when buying goods on specific e-shopping sites (such as E-bay).**

**Two alternative authentication methods of online banking based on 2-factor authentication were analyzed:**

## **Static password**

- **The most used authentication method (86% monthly plus).**
- **The perceived user friendliness (92%) of this method is high in Europe**
- **The level of trust is relatively high (74%).**

## **Dynamic password**

- **Is far less frequently used in Europe (56% monthly plus) than a static password.**
- **The user friendliness (77%) is notably lower in comparison with a static password**
- **The trust Europeans accord to a dynamic password (85%) is much higher than a static password (74%).**

**User friendliness should be bypassed to the benefit of trust for e-banking, as the dynamic password authentication method is more secure**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

- User identification methods for card payments
- User identification methods for e-payments
  - e-banking
  - **e-commerce**
- User identification methods for mobile payments
- Innovative user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

## 5. Recommendations to overcome the identified barriers

## ***From a security perspective, payments via TTP are the preferred payment scheme for e-commerce***

**On the Internet, card payment can either be:**

- **Direct from buyer to merchant (the transaction is not powered by an intermediary payment service provider, except the credit card company , e.g. Visa, Master Card)**
- **Indirect and relying on TTP<sup>(1)</sup> (i.e. electronic transaction where an intermediary payment service provider, such as Paypal or Ogone, secures the transaction)**

**Solutions where the payment is performed indirectly via TTP tend to take over solutions where the payment is done directly to the merchant. This observation is EU-wide and was quite expectable since the goods and services that are paid via e-payment methods are provided by EU or even world-wide merchants such as eBay.**

**TTP schemes appear to be candidates to the best payment schemes as they have two major advantages:**

- **The trust induced by the intervention of a well-known actor**
- **The privacy level offered to the buyer, since most of these schemes allow the buyer to communicate financial data only to a TTP and data related to the good purchased are only communicated to the merchant.**

(1) Trusted Third Party

## ***From a security perspective, 2-factor with a dynamic password is the best authentication method***

**In the context of e-commerce and Internet payment schemes, the TTP based payments schemes are better payments schemes than those not powered by an intermediary payment service provider:**

- **TTP evolve towards dynamic factor**
- **Direct payment to merchant stays static factor SSL based (with no other authentication than the card related information accompanied by the request for the related CvX numbers).**

**Independently of the payment scheme, from a security level perspective, the best user verification methods rely on 2-factor authentication systems (e.g. user ID + password, whether static or dynamic combined with the possession of specific device, card or security software).**

**However, most of the payments schemes today stay on a “1-factor” authentication systems (e.g. user ID + password).**

# ***Users prefer slightly the authentication directly with the merchant from a friendliness and trust perspective***

*It is not in line with the best authentication method from a security perspective*

**Payments for goods and services (not online banking) are seen as e-payment. Two authentication methods for paying online (with a credit card) were analyzed:**

**Authentication directly with the merchant**

- **Most frequent applications are specific e-shopping sites and downloading music**
- **Europeans find this method very user friendly (90%) and trustworthy (78%)**
- **Looking at socio-demographical factors, males tend to pay online directly with the seller more frequently than women, especially when they are shopping on e-websites**

**Authentication via a payment service provider (TTP)**

- **Mostly done on specific e-shopping sites. Compared to paying directly with the vendor, a far higher number of Europeans never use this kind of payment for various applications such as downloading music or booking a vacation**
- **Europeans find this method quite user friendly (80%) and trustworthy (76%), although to a lesser extent than paying directly with the merchant**



**User friendliness should be bypassed to the benefit of trust for e-commerce, as the authentication via TTP is made mostly with dynamic password which makes this method more secure**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

- User identification methods for card payments
- User identification methods for e-payments
- User identification methods for mobile payments
- Innovative user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

## 5. Recommendations to overcome the identified barriers

## ***From a security perspective, 2-factor authentication is the best authentication method***

**With regards to mobile payments, the most used user authentication methods are related to the use of 2-factor authentication combining usage of a PIN-code and possession of the mobile device.**

**However the sole reliance on the classic PIN-code protecting the mobile device is not to be considered sufficient to meet banking regulations “to know their customers”.**

**In the context of mobile payment schemes, the best user identification and verification methods are:**

- **based on the use of 2-factor authentication combining the possession of a (PIN-protected) mobile device and the use of a specific PIN code dedicated to the payment application**
- **delivered through a secure channel (e.g. through the use of bank card authentication in ATMs allowing mobile payment activation facilities)**
- **that were established based on a prior face-to-face authentication (e.g. opening of a bank account).**

**The required convergence and collaboration between financial services providers and the mobile operators is observed to either parcel out the market into multiple and often incompatible initiatives such as in France, or to federate the market around one (monopolistic) scheme as in Belgium.**

## ***User find the PIN code authentication method very friendly and trustworthy***

*It is in line with the best authentication method from a security perspective*

**Paying via the mobile phone is seen as something very convenient and user friendly. It is also more associated with a payment for small amounts.**

**Mobile payments are not linked with payments of large amounts or for very regular purchases.**

**Texting in competitions is the most popular application of mobile payment in Europe. Also frequently used applications are buying tickets (for the tram, the bus, etc.), downloading music and payment for automatic vending machines.**

**When payment via the mobile phone is authenticated by means of a PIN code, Europeans tend to rely on this method as the level of trust is quite high (76%).**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

- User identification methods for card payments
- User identification methods for e-payments
- User identification methods for mobile payments
- Innovative user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

## 5. Recommendations to overcome the identified barriers

## ***eID would be a real alternative authentication method provided that some barriers are overcome***

The electronic Identity card (eID) is another new tool on the market to support user authentication, which tend to widely spread within the EU population and become well-known to the citizens.

In some countries the issuance for these eID cards is fully managed by the governments (acting as a TTP), whereas in other countries, they result from Private Public Partnership (PPP) between banks and governments as issuing bodies.

There is a real interest of the banking sector to work with public authorities in matters of user authentication and e-signatures, and especially on the basis of eID cards which are powerful tools brought in the hand of the masses by the authorities "for free", as far as it concerns the banks<sup>(1)</sup>. In addition to the intrinsic security added value, these tools can even be seen as a marketing advantage for the payment scheme providers (e.g. Keytrade bank).

However some barriers to the use of (eID) QES signatures by the banks are identified, which prevent to use it today as alternative authenticating method (e.g. 3D-Secure):

- Lack of cross-border PKI interoperability and mutual recognition
- Liability (e.g. in case of fraud) and control on the issuance issues in countries where the banks are not part of the issuing process of eID cards
- Co-existence of the EU Directive linked standards and Banking sector's standards that all need to be followed

The liabilities issues could be solved through legislation. The Cross-border and mutual recognition issues should be enhanced by 2010 within the i2010 programme.

(1) (or at least when they are not part of the PPP issuing the eID cards)

## **Contactless/RFID<sup>(1)</sup> authentication method needs to be further secured than it is nowadays**

*This authentication method is only applicable for proximity payments*

**Proximity payments are defined as those in which the local data exchange takes place between the customer handset and the terminal at the POS through Bluetooth, infrared, or RFID. These ways of working appear more and more in specific applications domains, such as parking meters, movie tickets, etc...**

**During the last years the usage of contactless technology for proximity payments has emerged. This new payment method have firstly been introduced in the U.S. but now also European payment schemes are considering them. From a user perception, 34% of Europeans find it appealing and 29% are willing to use it.**

**In most cases, a user verification method such as a PIN is not used in contactless payments. While very easy to use, these authentication methods have their limitations with respect to the type of payments it could be used for (i.e. small amounts). Because of the wireless technology it is possible to capture data from the card using powerful antennas without the user's authorisation and or knowledge.**

**Hence dedicated methods should be investigated to protect the contactless cards against these types of attacks (e.g. card shielding, card activation/ deactivation...).**

**But recently Near Field Communication technology is being introduced for proximity payments by means of mobile phones, which will create a user authentication method similar to those used in mobile payment schemes by the mean of a PIN code.**

(1) radio frequency identification

## ***Biometry is not a real alternative authentication method for the coming 5 years***

**From a user perspective, Biometry would be a popular new authentication method. It is considered the most appealing (65%) and the Europeans are also willing to use this method (69%) more in comparison to the other prospective methods.**

**But from a technology perspective, biometry is not currently used and is not expected to be a relevant prospective method for authenticating users in the coming five years due to the following facts:**

- **The lack of stability, difficulty of use, costs effectiveness**
- **It does not provide added value compared to existing solutions**
- **It seems not to fit the payment industry problem of user verification in a non specific context, in an open and interfering environment, with no possibilities to select or train users for well behaved usage**

**However, if these authentication tools are going to take more importance in the longer term<sup>(1)</sup> as being part of authentication protocols outside e-banking or e-commerce, they will be used as alternative authentication schemes (with the detriment of password-based techniques) . There are already PCs being provided with fingerprint as user verification and this could then be deployed wider for payment applications.**

(1) To what extent and speed these solutions will be adopted in Europe is difficult to predict accurately.

## ***iDTV will apply almost the same user authentication methods as the ones applied in e-payment***

**A new technology that could support cashless payments is the Interactive Digital Television (iDTV<sup>(1)</sup>). From a user perspective, 27% of Europeans find it appealing and 22% are willing to use it.**

**It is expected that iDTV supported payments will be very similar to Internet payments in terms of user identification and authentication methods. Only the interfaces towards the user would be different (i.e. the iDTV instead of classical browsers).**

**The iDTV authentication modules might also be used as authentication tool in the framework of e-payment:**

- There is indeed an authentication module within iDTV allowing further authorisation to access certain content according to the type of subscription of a particular user.**
- It seems that this authentication feature will not serve any other purposes, and e-payment in particular does not seem to be in the roadmap of iDTV.**
- However, since a set up box could be used as a payment terminal offering more security than an internet payment via a PC without a card reader, this alternative authentication method could be considered in the future for e-payments.**

(1) iDTV is not an authentication method but a payment method

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

- Perceived by users
- Legal
- Contractual
- Commercial

## 5. Recommendations to overcome the identified barriers

# *User perception barriers are caused by the perceived lack of security*

The perceived lack of security remains an important barrier from a user perspective and is caused by an emotional/rational point of view:

- **Anxieties driven by:**
  - The lack of personal contact and direct knowledge between the two parts (e.g. What is the identity of the recipient? How reliable is it?)
  - The perceived complexity and complicated nature of the technology involved and by lack of transparency of the process (e.g. What are the intermediaries and how is it going to work?)
- **Negative experiences (whether actual or imagined) without really serious consequences, which are linked to technological shortcomings that tend to be eliminated fast**
- **More serious consequences of financial damage to the user, which are more extraordinary:**
  - Medium-related problems: due to the presence of intermediaries, there is a certain level of worry. These intermediaries can be either technology or a certain service providers (e.g. TTP)
  - Human error: all situations when error is not due to ill functioning technologies but to humans handling the information (e.g. inserting wrong amount to be paid with credit card, not verifying signatures)
  - Reckless behavior on the part of the user (e.g. easiness to get credit and fall to into a spiral of debt)



- **Anxieties wear off as actual usage grows and these methods become more integrated into people's everyday lives**
- **The process of familiarization is aided by the increased user-friendliness and performance of technology in general**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

- Perceived by users
- Legal
- Contractual
- Commercial

## 5. Recommendations to overcome the identified barriers

# ***Legal restrictions and obligations are not considered as important barriers***

## **Legal restrictions may relate to the use of:**

- National registration number
- Biometric technologies
- RFID technologies
- Certain technologies in communication (e.g. use of cookies)
- Encryption technologies
- Certificates for electronic signatures

## **Legal obligations may relate to:**

- Strict retention obligations for communication data
- Specific rules for the storage duration of personal identification data
- Strict identification obligations for money laundering purposes
- Obligation to collect personal data although this would not be necessary for payment of the service
- Strict requirements in relation to trusted third parties in the payment process
- Stringent information/transparency duties towards the end user
- Stringent requirements in relation to the burden of proof for information duties or in case of fraud or repudiation/dispute of a payment transaction
- Stringent security duties

**It appears that there are not many real regulatory barriers to the use of available or prospective best technologies identified in this study.**

**The legal provisions on the sharing of liability between Electronic Payment Instruments (EPI) providers and card holders seem to be quite reasonable. Some of them are at first sight burdensome for EPI providers. Nevertheless, they actually create a lot of user trust in electronic and internet related payment solutions.**

**The legal provisions that are relevant for user identification and authentication seem to be rather narrowly tailored to protect against fraudulent actions. They do not differ significantly between the Member States and they do not seem to impact adversely electronic payments in a disproportionate manner.**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

- Perceived by users
- Legal
- Contractual
- Commercial

## 5. Recommendations to overcome the identified barriers

## ***Contractual restrictions are not considered as important barriers***

**Contractual restrictions may relate to:**

- **Contracts between merchants and Electronic Payment Instruments (EPI) providers**
- **Contracts between users and EPI providers**
- **Responsibility of the issuer of an EPI**
- **Responsibility of the holder of an EPI**
- **Responsibility of the merchant**

**Contracts between merchants and EPI providers commonly put the liability for proper identification of the card user on the merchant**

**Combined with the fact that the law usually regulates the maximum burden of proof that can be imposed on the user, this does not seem to adversely impact electronic payments. It may actually increase user confidence. Even where EPI providers push the user's contractual liability to the legal limit, this does not seem to cause users to avoid such EPI solutions.**

**A contractual barrier could arise if for highly secured payment mechanisms liability is imposed on a merchant in the same way as it is done for payment instruments simply relying on the user's signature.**

## ***Limitation of user responsibility should not stimulate less care of authentication credentials***

**When looking at the new Directive, one clearly sees a limitation of the end-users responsibilities.**

**This protection feeling can be seen as a positive signal to promote the use of cashless payments on one hand, but on the other hand this also leads to the consequence that end-users may be less concerned with security issues and become careless with its credentials.**

**This limitation on user responsibility has thus a positive aspect on the economical side by constituting an incentive to use e-payment, but at the same time negative side regarding the security.**

**To struggle against that kind of behaviour, the user awareness is really important, as well as the possibility to sue fraudulent or even "bad" use of credentials.**

**On the other end, that Directive goes with an incitation for the bank to increase the securing of the e-transactions, sustaining authentication of each principals in a transaction, helping thus to arbitrate litigation (thanks to enhanced non-repudiation features).**

# Table of content

## 1. Introduction

## 2. Executive summary

## 3. Conclusions on user identification methods

## 4. Identified barriers against development of card payments, e-payments and mobile payments

- Perceived by users
- Legal
- Contractual
- Commercial

## 5. Recommendations to overcome the identified barriers

# ***Commercial barriers comes from high cost of some technologies and the differences in national legislation***

## **Authentication directly with the merchant**

- **Commercial barriers to users' authentication means would arise if the financial risks are higher than the benefits.**
- **Commercial barriers may arise due to the complexity and cost of integration of certain technologies, such as 3D Secure or CVx2. This concerns in the first place the payment industry itself and, to a lesser extent, merchants. CVx2 is compulsory for French online sales sites, but it often remains optional in other countries. The CVx2 can be validated by the issuing bank when authorization is requested through an encryption process.**

## **Different national laws**

- **Specific payment related legislation as well as non-payment related legal provisions in Member States are mostly based on European Directives.**
- **Therefore, the applicable legal rules are harmonized to a great extent.**
- **Nevertheless, differences in national legislation resulting from a margin of implementation as well as differences in interpretation by competent authorities, may result in commercial barriers to the development of new secure identification technologies.**

## ***Commercial barriers affect mainly the EPI<sup>(1)</sup> technology providers***

- **From a user perspective:**
  - **The legal framework provides for a very strong protection, so that no commercial barrier would exist for the user.**
- **From an EPI provider perspective:**
  - **This level of protection may be found too strong. Nevertheless, this does not seem to create real commercial barriers in practice.**
- **From a merchant perspective:**
  - **The use of more secure e-payment instruments results in lower liability risks.**
  - **For merchants, commercial barriers could however still arise from unreasonable terms and conditions in contracts with EPI providers.**
  - **On the other hand, it may be assumed that EPI providers do not have a commercial interest in putting too much liability on the merchant.**
- **From the perspective of technological developers:**
  - **The differences in national legislation, especially data protection requirements, may impose a practical burden to the compliance of the technology in all Member States.**

(1) Electronic Payment Instruments

# ***Table of content***

- 1. Introduction**
- 2. Executive summary**
- 3. Conclusions on user identification methods**
- 4. Identified barriers against development of card payments, e-payments and mobile payments**
- 5. Recommendations to overcome the identified barriers**

# *The perceived lack of security and commercial barriers can be overcome by changing the legal framework*

## Identified barriers

- **Lack of security perceived by users**
- **Commercial barriers:**
  - **Caused by high cost of some technologies**
  - **Caused by the differences in national legislation**
  - **Affecting mainly the EPI technology providers**

## Recommendation for overcoming these barriers

- **Increase information sharing for preventing, reporting and punishing fraud**
- **Continue ensuring data protection in current and emerging payment technologies**
- **No need to reinforce the liability of the user or the merchant for current identification technologies, but well the securitization of transactions**
- **Establish harmonization and certification of identification/authentication technologies**
- **Make sure that registration process is made with due care by the involved parties**
- **Reassess the sharing of liability between involved parties for emerging identification technologies**
- **Make recommendations about the interpretation of the Data protection and Data retention Directives in the Member States**

# *Increase information sharing for preventing, reporting and punishing fraud*

Security related information to consumers

**It could be considered to introduce a more general legal obligation to communicate security related information to consumers using certain EPIs.**

**However, the absence of such legal obligation cannot be considered as a barrier to the use of secure EPIs.**

Notification mechanisms in case of fraud

**A general obligation for financial institutions to inform supervising authorities in case of fraud in e-payments, may be beneficial to the prevention of fraud.**

**Currently, it is likely that very little fraud-related information is published because of the possible damage to reputation.**

**A notification obligation leads to the adoption of enhanced security, which in turn means less security breaches and therefore a general increase of consumers trust in electronic payments.**

Punishment of fraud

**It is important to support the financial sector technical security means by a legal framework allowing suing and punishing identity thieves.**

**Help and recognition offered to victims is important too as identity theft may cause long term damages on a person.**

## ***Continue ensuring data protection in current and emerging payment technologies***

**Secure payment technologies should never lead to the collection of unnecessary personal data. The data minimization principle should always apply as it is important to keep on making possible anonymous e-payments.**

**The introduction of new technologies (e.g. based on biometrics or RFID) may be more difficult due to personal data protection requirements. In some Member States, prior authorization of or notification to the national data protection authority may be required.**

**However, these national requirements do not appear to create barriers to electronic payments. Once a certain technology is notified or approved in all Member States, it can be used by all EPI providers.**

# ***No need to reinforce the liability of the user or the merchant but well the securitization of transactions***

## **Liability of the user**

The current legal regime appears to adequately protect users in case of problem situations. Consumers show a reasonably high level of trust in electronic payments.

Therefore, it does not seem necessary to adopt additional legislation to deal with the legal obligations and responsibilities towards the user of other parties involved in e-payments.

Too many rules may also become a barrier. EPI providers and merchants from their side do not seem to feel hindered by the current legal regime.

## **Liability of the merchant**

There is no immediate need to regulate the contractual relationship between EPI providers and merchants in order to foster trust in electronic payments.

The fact that EPI providers typically lay a lot of liability with merchants, which is backed up by some national courts, does not constitute a barrier to secure user identification methods.

On the other hand, the more secure the EPI, the less liability the merchant will risk.

## ***Establish harmonization and certification of identification/authentication technologies***

**The financial industry wishes a high level of security. But except what is stated in the Directive, there is no legal framework today requiring specific security measures for e-payments.**

**Nevertheless, there are already some schemes in place such as:**

- the BCE recommendations from 2003 that can be associated with the implementation of the Directive**
- In particular, for card payments, the European Payment Council has chosen to use smart-cards and follow largely the EMV standard, with as prior objective, having the same EMV based implementation for everybody**

**Most of the recommendations are criteria are based on assessment to be performed by Accreditation/Certification bodies. Having a more harmonised way to organise authentication and security in general would certainly enhance the global level of security.**

**It is important to note that self regulation or regulation through national and central banks is expected to be the preferred and best supervision model. From a risk and security point of view, overall policies are not always beneficial. The EU Commission is expected to play a role whenever there are any legal obstacles to obtain for instance interoperability.**

## ***Ensure that registration process is made with due care by the involved parties***

The weakest step in the authentication process has been clearly identified within this study as being the registration step.

This is because all subsequent steps rely on this first crucial task: if someone managed to be enrolled under a fake identity, the registration process will furthermore reinforce the link between this person and his fake identity (by providing him with official credential validating initially corrupted information).

It must be noted that in some cases, the legitimate owner of an identity may pretend to have been impersonate in order to repudiate a transaction. On the other side, it is also important to provide the user with means enabling him to prove that he has been abused (otherwise nobody will use his card anymore).

In both cases, it is important to take care that the systems in place do not turn in means to sustain hackers. The vicious circle is that the most one imposes "trusted-true ID", the most it will become necessary for hackers to steal identities.

## ***Reassess the sharing of liability between involved parties for new technologies***

The identification requirements resulting from money laundering legislation serve a legitimate purpose and do not create barriers to the development of secure e-payment technologies.

The strict identification requirements imposed must only be complied with once by the financial institution. Merchants from their side must still identify users to avoid being liable for fraudulent transactions.

However, as technologies become more secure, merchants will have more difficulty spotting fraud. For users it will be more difficult to repudiate transactions carried out with secure EPIs but also to prove fraudulent use of their credentials.

Therefore, it may be necessary to closely follow up the development of new technologies and to reassess in time the sharing of liability between the parties involved in the payment process.

Also, security requirements will have to be higher for centralized databases with user identification and credential information. Such requirements result from general data protection legislation as well as from the Draft Payment Services Directive. Assessment of compliance with such requirements is up to national courts.

The involvement of trusted third parties ensuring separation between the identification and payment process is a good development and should be followed closely.

# ***Make recommendation on the interpretation of the Data protection and Data retention Directives***

**In relation to the retention of data, both restrictions and requirements may exist:**

- **As a result of legislation implementing the Data protection and E-privacy Directive:**
  - **Personal data may not be stored longer than necessary for the purposes of the processing**
  - **Communications data and related traffic data may not be stored without the users' consent, except under strict conditions**
  - **Traffic data may however be stored for billing purposes in order to detect and stop fraud**
- **As a result of legislation implementing the Data retention Directive and Money laundering Directives**
  - **Traffic data must be stored during a certain period of time by providers of publicly available electronic communication service and networks operators and ISPs**
  - **Financial service providers must keep identification records for 5 years**

**It is possible that different interpretations of the said directives in various Member States slow down the development of e-payment technologies, in particular due to legal uncertainty/different requirements in relation to traffic data retention obligations. By way of example, data retention obligations may be very strict if legislation implementing the Data retention Directive in a certain Member State is extended to information society service providers or when legal uncertainty arises as to what should be understood by publicly available services and networks.**

**Should this be the case, it may be useful to release recommendations on the interpretation of the said directives.**