

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

Executive Summary
November 2007

SIEMENS

SEALED
Trust Services Architects


synovate
Censydiam

THE HOUSE OF
MARKETING




time.lex
Dumortier - Somers - Graux


Security
4 Biz

Objectives of the study and its 5 work packages

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 which started in February and ended in November 2007 was coordinated by Siemens. It includes 5 work packages (WP) delivered by different providers 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 - *delivered by Sealed and Security4Biz* -
- **WP2:** Assessment of user friendliness of identification methods, including user barriers perception – *delivered by Censydiam and The House of Marketing* -
- **WP3:** Comparison of findings with previous study on user identification methods realized in 2003 – *delivered by Sealed* -
- **WP4:** Regulatory, contractual and commercial barriers assessment of best used identification technologies – *delivered by Timelex* -
- **WP 5:** Recommendations – *delivered by The House of Marketing* -

In particular the goal of 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. 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.



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**

Security has been reinforced since 2003 but two-factor authentication is still not generalized

The most generic change that may be noticed in the evolution since 2003 is that security has moved from a technical “nice to have” feature towards a major cornerstone for ensuring trust in cashless payments, partly due to the contribution of the media to put any fraud related events in the spotlights.

It is noticeable that fraud, without increasing drastically, has changed towards well-organised crime. But official attacks/fraud figures are difficult to obtain as banks prefer to preserve their reputation and are not obliged in some countries to warn their supervising overlooking organisation about fraud.

Nowadays, 2-factor based authentication schemes have become the necessary minimal level of security for web-banking, card and mobile payment instruments but are still not implemented everywhere:

- The migration from magstripe card to chip card is taking longer than originally planned by the major card schemes, due to the extension to the 24 European countries. The so-called hybrid cards (combining both magstripe and chip technology) have led to a number of new fraud cases
- Not all banks have enhanced yet the security level of their web-banking applications to a 2-factor based authentication scheme
- E-commerce remains unfortunately basically tight to a lower level of security. Still most of the schemes use basic SSL based systems only, with no other authentication than the card information and the related CvX numbers.
- A large volume of mobile payment transactions are based on SMS for which no additional PIN-code is required than the one protecting the mobile device. Fortunately the user authentication methods most frequently used are related to 2-factor authentication combining usage of a payment or application PIN-code and the possession of the mobile device.

Generally speaking for Europe, one can conclude that the change of the fraud nature and enhanced technical skills and organisation of the hackers seem to be adequately addressed by the increased security level of cashless payment instruments offered by the financial world. However two-factor based authentication is still not generalized and implemented by all players of the industry.

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



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

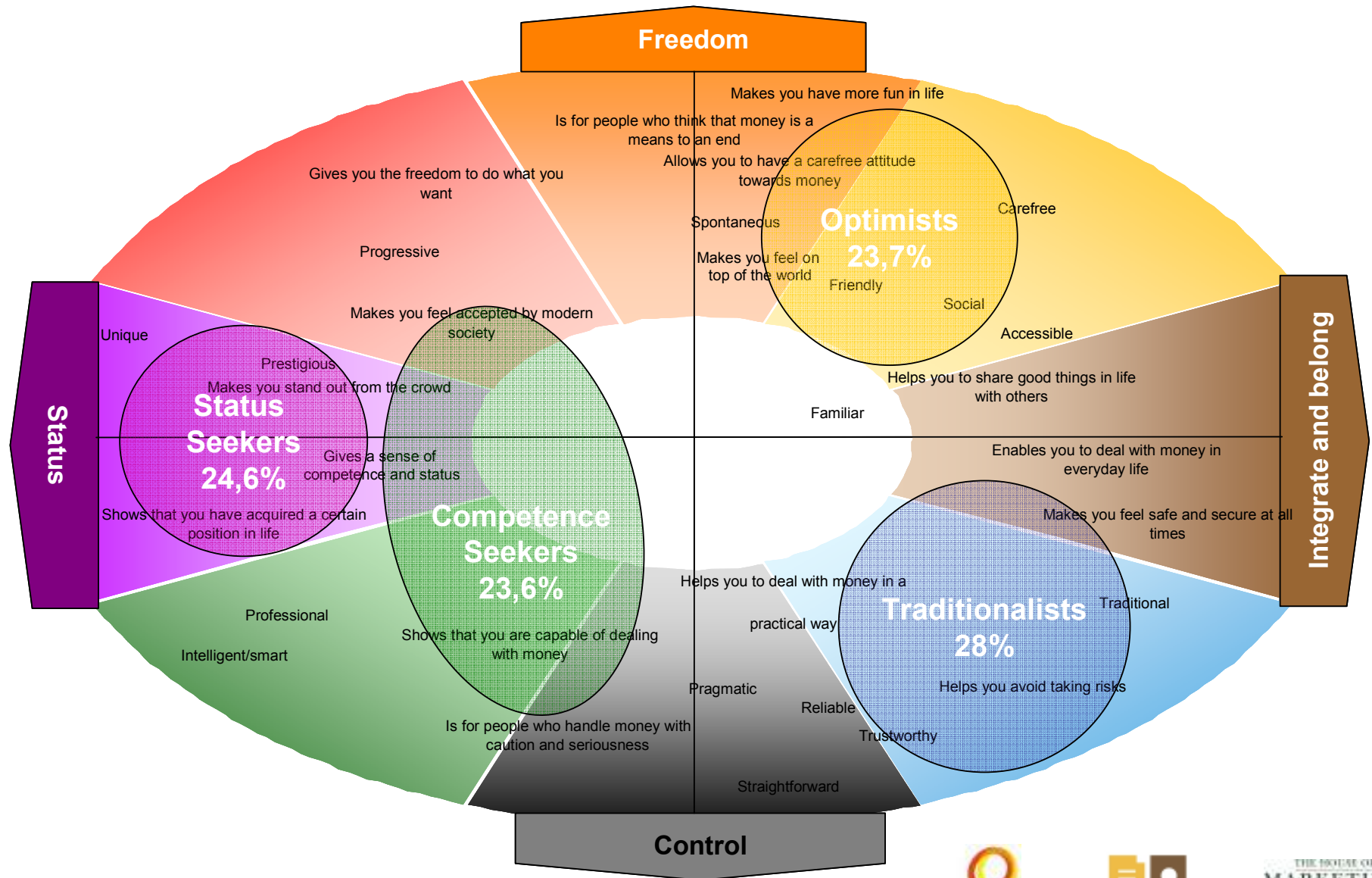
(1) at least once a month (daily + weekly + monthly)



Legend:



4 motivational user groups with specific expectations towards cashless payment solutions have been identified



Main barriers against the use of cashless payments in Europe⁽¹⁾ 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 details in the work packages.

Seven recommendations on the legal framework should be followed up to overcome identified barriers

- 1. 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
- 2. Continue ensuring data protection in current and emerging payment technologies**
- 3. No need to reinforce the liability of the user or the merchant for current identification technologies, but well the securitization of transactions**
- 4. Establish harmonization and certification of identification/authentication technologies**
- 5. Ensure that registration process is made with due care by the involved parties**
- 6. 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
- 7. 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**