CEPIS Position on
Authentication Approaches for Online Banking

1. Introduction

Performing financial transactions via an online connection to a bank or other financial institution is cheaper and faster than conventional means of conducting business. Yet despite the obvious advantages, there is still a reluctance to use it as the primary method of conducting business because of the risks associated with it. Consequently, banks are introducing new safety mechanisms to prevent attacks and increase trust. Besides the usual methods, additional ones are applied for authentication. As the voice of European IT practitioners and experts CEPIS is concerned that the use of security technology does not increase security but makes services less appealing to use. On the other hand, alternative approaches, which could raise security for users, are rarely employed if at all. Based on these findings, CEPIS strongly recommends that unnecessarily complex or cumbersome security technologies should not be applied. A cost-benefit analysis should be performed to assess the effectiveness of protection and the trade-offs for all parties involved.

2. Authentication approaches

The supply of online banking is increasing. Because banking activities are highly sensitive, higher security standards are required. In order to increase security, banks employ two-factor authentication, which involves something the user **knows** (e.g. password, PIN) and something the user **has** (e.g. smart card, other hardware token). Although the actual application may vary, most banks use the second authentication factor – a token that the user possesses. The types of authentication schemes can be classified as follows:

- a one-time password approach;
- a certificate-based approach;
- a timer-based (short) password approach;
- a certificate - smart card based approach.

The above approaches have their advantages and disadvantages. The trade-offs are often in the following areas:

- resistance against attacks;
- costs for the bank and/or the customer;
- ease of use;
- flexibility.

The approaches and their advantages are discussed in the CEPIS background paper. While the goal is to find a solution that is best in all dimensions, in most situations a prudent way to deal with the trade-offs is needed.

3. Trade-offs and how to deal with them

A typical trade-off is between the one-time password approach and the smart card approach. The one-time password approach is cheaper and less demanding, while the smart card approach is more robust against attacks. In this situation, a risk analysis must be carried out and a choice offered so that users can select the method that fits their preferences for potential risk and other factors.

4. Concerns

We recognise the dangers related to online banking. While some degree of imperfection will always exist, we are more concerned about the use of methods that do not improve security but make services harder to use. Some security measures do not raise the security level and only give an erroneous impression of security, while alternative approaches that could increase security are rarely used or not at all.

Consequently, we have serious concerns:

1. The tendency to use complex and error-prone security measures that do not provide any security improvement is an unnecessary burden that will discourage or prevent users from easily adopting electronic business in general; this conflicts with the European Union's goals for a common electronic marketplace.
2. Unfavourable media coverage of security measures may damage the reputation of all security endeavours, resulting in consumers' loss of confidence and trust in security technologies. Such distrust is damaging as it makes it more difficult to react efficiently to new security threats.

3. We are concerned about unprofessional behaviour demonstrated by not fixing evident shortcomings. We are worried about the damage that such behaviour might cause to the public's view of the ICT profession's reputation.

5. Recommendations

Recognising the importance of online access as one of the vehicles for the development of cheaper, faster and more reliable services, we have identified areas of improvement where all parties involved should endeavour to deploy services without unnecessary or excessive risks. Based on the findings of our professional working party, CEPIS has formulated recommendations to four groups of stakeholders, namely:

1. banks and other financial institutions and organisations;
2. governments and regulators;
3. professionals and
4. customers.

5.1 Recommendations to banks and other financial institutions and organisations

We strongly recommend that unnecessarily complex or forbidding security technologies should not be used. Instead, a cost-benefit analysis, covering primarily the following points should be carried out:

1. an assessment of the effectiveness of a planned protection compared to the existing one;
2. an assessment of burdens for all the involved parties.

Customers should be informed of the risks, existing security measures and of their rights in case of fraud. Banks should inform their customers of their rights and of the help available to compensate for their loss in an easy-to-understand manner such as e.g. air travellers have in all EU airports. Customers should also be given the choice of different methods for authentication and be able to select a system that matches their approach to risk and their preferences.

Financial institutions and organizations should inform their customers that security measures on their computers are vital for secure online banking and that security must be constantly maintained.

In case of fraud, the bank should offer all possible assistance to the affected party, especially as the capabilities of a bank considerably exceed those of a citizen.

No practitioner should be considered as qualified to work for a bank or to provide services to a bank without being a member of a professional association that has adopted a code of ethics.

5.2 Recommendations to governments

Where existing laws are not sufficient, legislation should be put in place to protect customers in cases of online banking frauds and to compensate for customers' losses in proportion to the adequacy of the bank security measures.

Customers should not be the only ones to carry the burden of the consequences of criminal acts related to online banking, especially if such acts are facilitated by (insufficient) bank security measures.

Legal obligations should be put in place to inform customers of existing security measures and of their rights in cases of fraud.

5.3 Recommendations to professionals

We encourage professionals to uncover the problems of inadequate security technologies and work towards fixing these problems.

Professionals should decline to provide their services to banks in certain cases, for example when the cost of bank transactions is not transparent, transactions are vulnerable and when there is a possibility of personal data being disclosed.

5.4 Recommendations to customers

Customers are encouraged to enquire about security measures and to read the small print of the conditions of services. They are encouraged to consider the security of their electronic transactions when choosing the bank, not simply to opt for the cheapest offer or for the most aggressive marketing campaign.

Customers should continuously maintain the security of their computers in order to support secure online banking.