Evaluating the Security of Electronic Money

Simon L. Lelieveldt[i]

After defining electronic money it is explained that the Dutch policy stance with respect to electronic money is that issuing value is seen to be equivalent to deposit taking and therefore subject to supervision. As a result the Dutch central bank actively monitors developments with respect to electronic money and reviews the schemes under the rules of the supervision law. The most important findings of the BIS-report on security of electronic money are summarized and an overview is given of issues that could be studied as a part of the review of an electronic money scheme.

1 Electronic Money

In this paper, electronic money will be defined as the electronic representation of pre-paid value on a device. This definition excludes paper-based payment instruments and payment methods in which the customer is being debited after the actual purchase. The definition allows for a wide variety of legal qualifications of the prepaid value[ii] and allows the value to be represented in different formats, such as balances, coins or a combination of both. Furthermore, the definition does not restrict electronic money to smart cards or computer disks; it allows for the value to be represented on a wide variety of electronic devices, including cellular phones or mainframes.

2 Regulation of Electronic Money

In the Netherlands, legal opinions have confirmed that issuing multi-purpose prepaid cards and network money are equivalent to deposit-taking. This means that issuers of electronic money need a banking licence and are subject to supervision. This policy should not be understood in the sense that the central bank is limiting the issuance of prepaid cards to existing credit institutions. The deputy director of the central bank, van der Wielen, has explained this during a seminar on electronic money on February 4, 1997.

> *"The market is also open for those who are prepared to establish a bank or to involve a bank in the project in such a way that it bears full responsibility for the money flows involved."* [iii]

In other words, the requirement that banks should issue the value does not necessarily imply that the scheme operator should be a credit institution. It does imply however, that any non-banks involved in the scheme, will have to comply with the relevant requirements of the central bank, which will be passed on from the participating banks to these organizations.

As a result of its supervisory role the Dutch central bank actively monitors developments with respect to electronic money and reviews the schemes under the rules of the supervision law. The following paragraphs intend to provide some insight in the way such activities are performed.

3 Security of Electronic Money

In August 1996, the Committee on Payment and Settlement Systems (the CPSS) together with the Group of Computer Experts (GCE), based at the Bank for International Settlements (BIS), published their report on the security of electronic money.[iv] The relevance of this report stems from the fact that the CPSS serves as a forum for the central banks of the G-10 countries to monitor and analyse the developments in payment systems.

The report has been drafted on the basis of interviews, conducted in the first three months of 1996, with a large number of suppliers of electronic stored value products. The interviews focused on the security aspect and especially on the innovative elements of these products: the pre-personalization and transaction phase of the life-cycle and the physical security of the devices used. For a good understanding of the findings in the report, it should be noted that most electronic money products, at that stage, were card products and were still in a pilot phase. The findings cover the content of the security-measures on the one hand and the process of designing and implementing these measures on the orther hand.

As for the content of security measures the report concludes that measures exist to design and operate electronic money schemes that are at least as good as the current payment instruments. These schemes may include the use of an unsafe medium such as Internet. It should however be understood that every single scheme has to be judged on its own merits. There is no ‘magic bullet’ in the form of one universally applicable security measure that will make a system safe. It is always the combination of security measures, with respect to both design and exploitation of the system, that will determine whether a system will actually be sufficiently safe.

With respect to the process of designing and implementing security, the report notes that a real top down approach of security has proved to be rare. Most of the suppliers gradually developed and improved their security-policy, risk-analysis and implementation of security measures. Of course, the fact that most schemes were still in a pilot phase has influenced this observation. Nevertheless, the report states that an integrated, overall risk-management approach to security, including independent security assessments, is an important component of the security. As for reviewing the security of schemes, the report suggests that these should not be limited to the design of the system, but that these should also include the actual implementation of that design and the use of external independent security experts.

4 Evaluating the Security of Electronic Money

In the Netherlands, issuers of electronic money are subject to supervision, based on the Act on the Supervision of the Credit System (1992). A special evaluation framework has been developed in order to encompass the specific aspects of an electronic money product (legal, technical, financial, organizational, security). The review is being performed by a multidisciplinary team of experts. As a basic principle, each aspect of the review must be assessed by two experts to limit the effect of personal judgment biases.

In practice, the evaluation of the security of electronic money products can be performed by establishing:

- the commitment of management with respect to the content of the security policy and the risk analysis,
- the fact that security is a separate organizational responsibility and that relevant reviews and policies are periodically being updated,
- the content of security policy,
- the actual implementation of security policy through all relevant controls,
- the soundness of the designed protocol, preferably also reviewed by an external -cryptographic- expert,
- the content of the security risk analysis of the design and operation of the electronic money scheme,
- the content of emergency or fallback scenario's,
- the fact that security requirements and controls extend to external organizations as well.

Some of the criteria that are relevant to establish the soundness of the designed protocols are:

- each technical entity should authenticate another entity on the basis of common (internationally standardized) cryptographic techniques. It must be demonstrated how the mutual authentication works and is implemented,
- communication between entities (chipcard, hardware and central computers) should be secured. Security information should be encrypted. It must be indicated how this communication security works and how it will be realized,
- it must be impossible to use non-authentic devices and hardware. Use of such equipment should be detected immediately. Measures and detection mechanisms must be described,
- it must be impossible to manipulate the content of the chipcard (notably with regard to value, PIN/password and keys). Measures and detection mechanisms must be described,
- a 'hard' security feature should be implemented with regard to payment functions, if various services are offered through the chipcard. Measures and the detection mechanism should be described. Involved institutions must show that they have ascertained that the devices and hardware used are secure.

One might wonder if it were possible fullfill the above criteria and develop a new electronic money scheme at the same time, since in practice it can be observed that policies, procedures and practices are somewhat unstable during the development and the initial pilot phases of a product. It could therefore be considered to use different requirements for mass-market products and products in a pilot stage.

---

[i] Senior Policy Planner, Payment Systems Policy Department of De Nederlandsche Bank. The views presented in this paper do not reflect in any way a formal position of De Nederlandsche Bank.

[ii] See: The Task Force on Stored-Value Cards of the American Bar Association, A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money, The Business Lawyer, February 1997, Volume 52, Number 2.

[iii] See: Henny van der Wielen, Deputy Director of the Central Bank of the Netherlands, Electronic Money: A European Perspective, Address Before the London Bankers Club (Feb, 4, 1997).

[iv] Committee on Payment and Settlement Systems & Group of Computer Experts, Central Banks of the Group of Ten Countries, Bank for International Settlements, Security of Electronic Money, Basle, 1996, see:http://www.bis.org/pub/cpss18.htm.