What will the Electronic Euro look like?

Berry Schoenmakers

DigiCash bv

Financial institutions have been processing transactions electronically for several decades now. Two important developments that will open up the field of electronic payment systems are now taking place. First, the prospect of electronic commerce over the Internet is creating a large demand for electronic payment methods for an open network. Second, the introduction of nation-wide electronic purse schemes is creating many more places and situations where smart cards can be used for cost-effective off-line payments. But to what electronic euro are they to converge?

Introduction

With the introduction of electronic devices that carry digital representations of money, it is clear to the general public that electronic cash systems are becoming a reality. Examples of such devices are telephone cards, smart cards, and PCs connected to networks. Although technically speaking there are many differences with ordinary cash, these *prepaid* payment systems are conceptually closest to what people view as the electronic equivalent of cash. On the other hand, banks and merchants have been processing payments electronically already for a few decades, and created very convenient - for some people too convenient - credit cards as well as the more recent debit cards. In credit and debit payment systems, which are also called *payment by instruction* systems, money is basically moved from one bank account to the other. Consequently, any such payment by instruction needs to cleared on-line with the bank or credit card company in order to prevent discrepancies between accounts.

Given the prospect of electronic commerce over the Internet, many parties would like electronic payment systems suitable for use over open networks to become a reality soon. This will be quite an achievement, since traditionally banks, multinationals, and larger organizations have been using private connections and closed networks to do such business. Electronic commerce over the Internet will also partly replace the huge volume of business that is now being conducted by phone and by fax. Then there are the cable networks which are also being prepared to pave the way for electronic commerce (where people will be using their so-called "network computers"). And, once electronic commerce has been spread to all these networks, soon customers will expect that these systems are again integrated with the systems that are in use in the shopping malls.

A plethora of electronic payment systems for use over the Internet is currently being proposed, designed and implemented. The main reason why the introduction of these systems is not happening overnight is that the enabling technologies themselves are still in the process of maturing. For instance, cryptography and public key cryptography in particular are widely recognized as such an enabling technology. Although the notion of digital signatures has been around now for over twenty years, large-scale application has only taken off recently since public key certificates are incorporated in the latest web browsers (e.g., to certify software downloads). Apart from providing basic security mechanisms that make the use of open networks viable, cryptography is also at the heart of the monetary system itself, as we will see below. Other important enabling

technologies are tamper-resistant smart cards equipped with sufficient memory and crypto co-processors, all kinds of personal computing devices with user-friendly interfaces, and convenient network protocols.

Payment by instruction systems

Several major credit card companies have united their efforts in the SET (Secure Electronic Transaction) proposal. The SET proposal derives from the iKP payment scheme proposed by IBM [1], and was first adopted by MasterCard and later by VISA as well [6]. Since SET is now supported by major software companies, it is currently the de facto standard for credit card transactions over the Internet. SET allows for several security levels. In the short term this means that the security will rely on the fact that digital signatures are used for authentication (more accurately, for non-repudiation of origin), thereby replacing the use of ordinary signatures, and the use of public key encryption to protect the use of credit card numbers and other transaction details. Since application of public key cryptography only makes sense if there is an infrastructure for certifying public keys, a great deal of the SET proposal is devoted to the specification of a hierarchy of certification authorities.

The main reason why the introduction of electronic payment systems is not happening overnight is that the enabling technologies themselves are still in the process of maturing.

Of course, there will be a huge market for SET, and it will replace many transactions which are now done routinely by telephone or fax (on a global scale). But there are also some obvious disadvantages. For small purchases in the range of a few cents to several dollars, the use of credit cards is at present not cost-effective. Also, peer-to-peer payments are not possible because only merchants can receive payments, and many people simply do not have or get a credit card.

Similarly, network payment systems for use with debit cards and prepaid cards, as well as systems for electronic cheques inherit their properties. For example, the Chipknip and the Chipper will both be usable over the Internet, but receiving money will therefore be limited to merchants again. A technical reason for this is that these systems rely mostly on symmetric cryptography (like DES), which requires that both payer and payee share the same secret key. A straightforward solution is to give all users the same secret key, but this is generally considered insecure, as this would mean that breaking a single smart card (i.e., extracting its secret key) will suffice to break the complete system. The standard solution is therefore to break the symmetry between payers and payees by equipping the merchants with a highly tamper-proof box called a SAM that contains a masterkey. The users' keys are derived from this master key in a process called diversification by applying a cryptographic hash (e.g., SHA-1) to the concatenation of the master key and the user's card number. The idea is that the SAM is more difficult to break than a smart card, and also that it is possible to routinely check the SAMs (as part of the maintenance) if they have not been tampered with.

Electronic cash

At DigiCash [4] we are developing electronic equivalents of cash. In these systems, we are not only using public key cryptography to enhance the security in general (e.g., for non-repudiation), but also at the heart of the system by using some form of digital signatures to represent the money itself. The idea is that by providing electronic coins some useful properties of ordinary cash are inherited. For example, because coins are publicly verifiable, any user can verify the authenticity of a coin. Small purchases, requiring only one or a few coins, are simple and efficient.

Security-wise, the nice thing about electronic coins is that no party except the bank (or rather the ecash mint as we sometimes prefer to call it) is able to create coins. Hence, the only way to attack the system is to duplicate coins that are already in circulation, but this is easily stopped by keeping track of spent coins. To some extent, it is true though that to achieve these properties, it is not strictly necessary to resort to the use of electronic coins. To intrinsically protect the privacy of the users, however, electronic coins are the only way to go.

In fact, what we do is to take full advantage of public key cryptography, which is required anyway to achieve a high-level of security. The ecash^{TM} system shows that this can be done in a practical way. Ecash users connect their computer to the Internet, where they obtain electronic coins from ecash issuers, store them on the hard drive, and later spent these coins at ecash shops that present themselves on the Internet. However, it is also possible to pay just any other user (peer-to-peer payments), and, if desired, it is even possible to include the payment in an e-mail. In all cases, the property of finality is achieved, which means that the money will be in the account of the payee as soon as the payment arrives (and is found valid).

Ecash finds its roots in the work by Chaum on elec-

e	3	5	7	11	13	17	19	23	29	31	37	41
D_e	$0.005	$0.01	$0.02	$0.04	$0.08	$0.16	$0.32	$0.64	$1.28	$2.56	$5.12	$10.24

Table 1: A binary scheme with k = 12 different denominations

tronic cash [2], who invented the notion of electronic (or digital) coins as well as the basic protocols for electronic cash. Electronic coins possess similar properties as metal coins, among which is the unique feature that a payment transaction leaves no trace about the identity of the payer. Currently, ecash technology (as provided by DigiCash [4]) is used by a number of banks around the globe. As an example, Figure 1 shows a snapshot of the Deutsche Bank ecash client. These banks issue ecash to their customers, who can then spend it at affiliated merchants on the Internet.

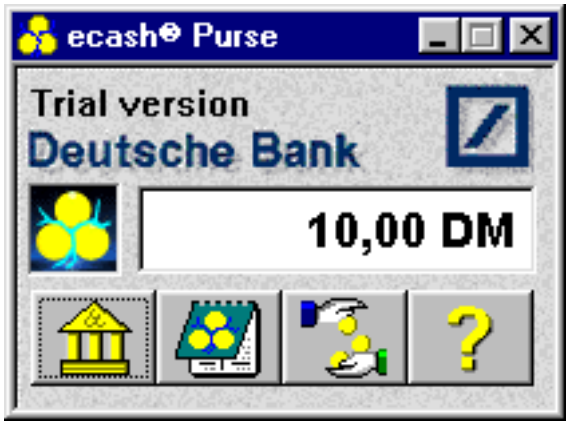

Figure 1 Deutsche Bank ecash client

Ecash coins are in fact a specific type of RSA signatures. For each generation of coins the ecash mint uses an RSA key consisting of a public modulus N, the first k odd primes as public exponents $\{e_i\}_{i=1}^{k} = 3, 5, 7, 11, \ldots$, and the corresponding private keys $\{d_i\}_{i=1}^{k}$. Each exponent e corresponds to a denomination D_e, see Table 1 for an example. Each private exponent d_i is determined from the factorization $N = pq$, which is kept secret by the mint, as the multiplicative inverse of e_i modulo $\phi(N) = (p-1)(q-1)$. We denote the inverse by $1/e_i$. In order that the inverses exist, the RSA modulus must satisfy that each e_i is co-prime with $\phi(N)$, that is $\gcd(e_i, \phi(N)) = 1$, for $i = 1, \ldots, k$, which is not a severe restriction. Then we have that $m^{d_i e_i} \equiv m (\mathrm{mod}\ N)$ for all $m \in Z_N$, which is the basis for RSA signatures.

An ecash coin C of denomination D_e is an RSA signature of the form

$$C = f(x)^{1/e} (\mathrm{mod}\ N)$$

where x is a randomly selected coin number, and $f(x)$ denotes a suitable redundancy-adding function, which we do not further specify here. Verification of a coin C proceeds by computing $C^e (\mathrm{mod}\ N)$ and checking whether it is of the form $f(x)$ for some x. In this way, we take full advantage of the message recovery facility of RSA signatures, and storage at the client side for a coin is equal to the size of the modulus (say 96 bytes). At the mint only the coin numbers need to be stored (to stop double-spending), which can be as low 10-20 bytes per coin.

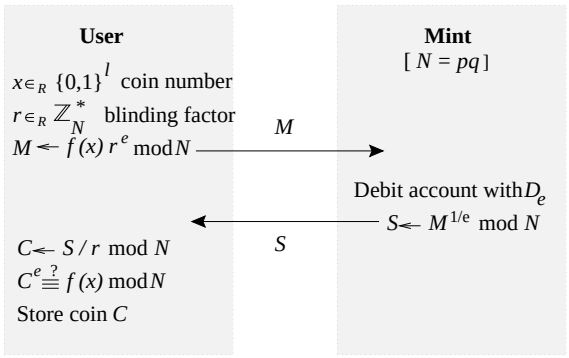

Figure 2 Withdrawal of a coin

Coins are obtained in special blind signature protocol [2]. It consists of two moves as shown in Figure 2. In practice, this protocol is run in parallel for a bunch of coins. The unforgeability of ecash coins relies on the security of the RSA cryptosystem, which is widely believed to be unbreakable when primes p, q are both a few hundred bits each. That is, no easier method than factoring the modulus N has been found to break these systems, and therefore this task is considered infeasible.

By the properties of the withdrawal protocol, any coin C in a certain execution of the protocol could just as well be received in any other execution of the protocol (for the same denomination). Therefore, ecash coins are *unlinkable*, which in turn ensures that no two payment transactions originating from the same user can ever be recognized as such. This is a very strong notion of privacy, and at least ensures that the coins themselves leave no clue to the payee about the user from which the coins originate.

To appreciate the strength of unlinkability let us put it in contrast with a weak notion of privacy based on pseudonyms. Consider the following scenario. When you buy a prepaid telephone card you can do

this completely anonymously at a newsstand (paying cash). Later when you use the card in a public phone the telephone company will have no clue that it is you making the phone call because you bought it anonymously. That is, the individual telephone calls are untraceable, as they cannot be connected to your identity. Suppose however that the telephone company gives every card a unique number, which is quite realistic as this is a basic mechanism to detect fraud (i.e., to find cards on which the total spent is larger than the card's value). Then it is easy to keep a file per card of all phone numbers called from that card (and possibly the time and date of the calls as well). Since a similar file is kept per home-phone as well, a simple pattern matching procedure will in many cases reveal the identity of a card's owner. Thus, although the card is obtained anonymously (and the card number acts as a pseudonym), the identity of the card's owner can be revealed anyway because all calls from the same card are linkable.

Conclusion

In building a practical payment system such as the ecash^{TM} system we use a lot more cryptographic techniques and security measures than considered above. Still, ensuring security of a payment system is only a small part of the actual implementation work. Many interesting techniques from the field of transaction processing [5] are applied to make communication between clients and servers reliable and to make programs fault-tolerant. And, in general, adequate software engineering is required to make it all work.

Currently, payments are cleared on-line with the ecash mint to prevent that coins are double-spended (clearly coins can be copied). The next step will be to use smart cards (equipped with a crypto co-processor) to build a system in which double-spending is impossible, because smart cards are assumed to be tamper-resistant. A fallback mechanism ensures that smart cards that have been tampered with can be traced - without sacrificing privacy for smart cards that are being used properly (see [3] for the basic principle of off-line electronic cash). Integrated in an electronic wallet, this will be a very convenient way to spend your electronic euros, either in a shopping mall or over any open network.

References

[1] Bellare M., Gray J., Hauser R., Herzberg A., Krawczyk H., Steiner M., Tsudik G., and Waidner M. *iKP - a family of secure electronic payment protocols.* In First USENIX Workshop on Electronic Commerce , 1995.

[2] Chaum D. *Blind signatures for untraceable payments.* In D. Chaum, R.L. Rivest, and A.T. Sherman, editors, Advances in Cryptology - CRYPTO '82 , pages 199--203, New York, 1983. Plenum Press.

[3] Chaum D, Fiat A., and Naor M. *Untraceable electronic cash*. In Advances in Cryptology - CRYPTO'88, volume 403 of Lecture Notes in Computer Science, pages 319--327, Berlin, 1990. Springer-Verlag.

[4] DigiCash http://www.digicash.com .

[5] Gray J. and Reuter A. *Transaction Processing: Concepts and Techniques.* Morgan Kaufmann Publishers, San Francisco (CA), 1993.

[6] http://www.mastercard.com and http://www.visa.com.

At DigiCash bv, Berry Schoenmakers is involved in the design and implementation of electronic payment systems, which includes many cryptographic and security-related aspects. Before joining DigiCash in 1995, he worked for three years in the Crypto group at CWI (Centrum voor Wiskunde en Informatica), where he was involved in the CAFE project. He received MS and PhD degrees in Computing Science from Eindhoven University of Technology in 1988 and 1992, respectively.