



The Long Road to €ldorado

Electronic transactions can be made using a wide range of processes — some successful, others less so. In fact, companies are still investigating what form of digital money will be most acceptable to customers, how best to encrypt personal data, and which standard is likely to gain worldwide acceptance.

By the end of the 1990s, digital money seemed headed for a bright future, largely at the expense of bills and coins. Bank experts were already beginning to think up ways of how to control money supply in an economy in which cash would become peripheral (see Interview, page 44). But the initial euphoria has subsided. Although new electronic payment systems are continually finding their way to market, no system has made a breakthrough. For a while, it looked as though “eCash” — the successor to “DigiCash” — would make an impact on the German market. Although the digital money system from eCash-Technologies was backed by institutions such as Deutsche Bank, it never really caught on with customers and was discontinued in May of this year.

“Technologically speaking, it was a highly sophisticated process,” says Dr. Joachim Henkel from the Institute for Innovation Re-

search and Technology Management at the Ludwig-Maximilian University in Munich. “But it was too complicated.” People wanting to use the system to pay for goods online first had to identify themselves at the post office. Then they had to install special software, file a digital certificate and generate digital coins, which they sent to the bank. The bank validated the coins by debiting a corresponding sum from the user’s account and then sending the coins back. Basically, potential users had better things to do and gave the new digital money the cold shoulder.

A similar fate befell “CyberCoin,” a rival product to CyberCash GmbH, at the end of 2000. Once again, the procedure was too complicated. “Customers will only go to such trouble when they know that they are using an accepted form of payment,” says Henkel. “People just aren’t prepared to go through a complex procedure every time they want to

purchase something online.” Henkel also claims that most people don’t understand how digital money works. That’s not so surprising given that electronic money on a hard disk remains an exotic idea for many of us. Correspondingly, most e-commerce purchases in Germany still involve such standard procedures as cash on delivery or payment on account. Indeed, while U.S. and British citizens use credit cards to pay for 95 percent of all purchases on the Net, Germans tend to stop an online transaction when asked to enter a credit card number.

One reason for this is anxiety about the safety of using credit cards for online purchases. According to estimates by the EU Commission, card fraud cost 600 million euros last year. Eurocard, a German credit card company, claims that the level of fraud in the Internet is ten times higher than in the rest of the market. That’s why online purchasers often see an onscreen symbol representing a key or a lock — a sign that the data will be encrypted. In particular, the large online outlets provide SSL (secure sockets layer) encryption for online payments. This creates a relatively secure link, inaccessible to third parties, between the server and the customer’s PC. However, even this system has a substantial drawback: online traders have no way of checking whether customers have really entered their own personal data.

Customers wishing to use the SET (secure electronic transaction) standard as developed by Visa and Mastercard must first obtain certification from their own bank. This comes in the form of a special encrypted electronic wallet, which is sent to the online outlet to pay for goods. With the current version of the SET standard, the electronic wallet is stored on the customer’s PC. In the future, however, plans call for this to be administered on a secure server. An even safer option would be to place the wallet on a special chipcard (SmartCard). But users would then need a card-reader, which currently costs around 100 euros. “The security argument alone isn’t enough to persuade people to buy one,” says Knud Böhle, who monitors the development of electronic payment systems internationally at the Institute for Future Technological Research in the →

Spanish city of Seville. "Customers aren't ready to pay for a card-reader yet." Henkel is also skeptical. "Most people wouldn't even know how to install one," he said.

Nevertheless, Böhle believes that SmartCards will boost online business in the medium term. His optimism is based on the fact that planning for the introduction of such cards is well underway. By 2005 at the latest, all credit cards will be fitted with microchips for encrypting data. "That will give people an

incentive to install a card-reader in their PCs," says Böhle. He also believes that the government could promote acceptance by allowing people to sign their tax returns with a digital signature and submit it by e-mail.

German legislation on digital signatures has already created the basis for online dealings with public authorities. A 1997 law was conceived to give digital signatures the status of a supplementary ID card. In May 2001, German law was modified to conform to EU guidelines introduced in January 2000 for a European-wide standard in this area. Use of an electronic signature, for example, makes it possible to determine whether a text has been manipulated during its journey through a data network. However, hackers still manage to crack even the most secure software with the help of so-called Trojan Horses. Therefore, it will be some time before you can send your attorney sensitive documents via e-mail.

Paying small amounts of money via the Internet is much less problematic. Indeed, as soon as PC-based card-readers become standard, special cashcards will provide a convenient way of making "micropayments." In Sweden, Finland and Belgium, for example, it is already possible to reload a SmartCard via the Internet and then use it for online purchases. In contrast, this feature is barely used in normal retailing in Germany, where some 20 million cards with a rechargeable wallet function are in circulation. Part of the problem is that too few outlets accept the cards, and with 20 different, incompatible systems throughout Europe, standardization remains a problem. For instance, it's impossible to reload a German card from a Spanish cashcard terminal — a frustrating experience for tourists.

Experts are forecasting a bright future for billing systems. Here, users first install a special software program that enables them to make small payment transactions using a computer mouse. "The amount is then charged to the customer's telephone bill, to the bill from their Internet provider, or to some other established account," says Böhle, adding however, that "New firms are at a disadvantage here, since they first have to develop a relationship with the customer." Such a billing system is offered by In Medias Res.

The company's product, Net900, is licensed to Deutsche Telekom, which uses it under the name of Click & Pay net900. Even simpler are prepaid Internet cards such as the "Paysafecard," which is designed to make online payments not only safe but also anonymous. Not surprisingly, such cards are principally used to pay for Internet pornography. As a rule, the cards incorporate a secret number, which users first have to scratch free. This is then entered into the online payment form. A PIN code is also required in some cases. The central computer at Paysafecard checks to see if the balance credited to the secret number covers the purchase. This fall, DeTe CardService, a Deutsche Telekom subsidiary, will launch a rival card known as "MicroMoney." But such payment systems have a big drawback, as card suppliers generally charge online retailers a fee of five to 35 percent per transaction.

In the future, cell phones could also replace small change. In Finland, they can already be used to purchase drinks from vending machines or to pay at the laundromat. There are also various cell phone-supported payment procedures in Germany. With the "Paybox" system, for instance, customers provide their cell phone number with their order. The retailer communicates this number and the amount due to Paybox. Within seconds, the customer receives a call and is asked to enter a PIN code to confirm the purchase. Finally, Paybox withdraws the sum from the customer's account and transfers it to the retailer. Here again, too few retailers have shown an interest in using the system.

Meanwhile, engineers continue to work intensively on new systems. In France, some cell phones from Motorola and Sagem are fitted with a second slot for a special chipcard to be used for payment. Another variant has the SmartCard already integrated into the cell phone. Böhle is now working with Visa and Nokia to test such a model. "If we can speed up the payment process and increase the number of businesses that accept the system, cell phones could become an everyday method of payment," says Böhle. "One day, we'll be able to transfer money simply by pushing a button." *Güven Purtul*

Money Talks

The old expression "money talks" is truer than ever. A split second after you drop a coin into one of the latest pay phones or vending machines, it tells it all. Size? Weight? Magnetic properties? Speed? Impact sound? You name it. In all, explains Francisco Ibañez, R&D Director of Siemens Elasa in Zaragoza, Spain, the world's biggest producer of public telephones, coins have to run a gauntlet of 22 validation parameters before passing muster. That may sound pretty tough, but counterfeiters still aren't licked. Now, with the impending introduction of the euro — probably the most technically advanced metal currency ever produced — and a new system from Siemens Elasa that updates the coin validation software in public phones, counterfeiters may finally have to call it quits. The 1- and 2-euro coins, for instance, will have such a complex inner structure that, once dropped in a pay phone, their unique signatures will be nearly impossible to duplicate. Great, but how are telephones that are used to gulping Deutsche Marks and Drachmas suddenly supposed to acquire a taste for eu-



Tomorrow's pay phone. Siemens Elasa is now testing its WebPhone. Outfitted with a 12" tempered glass monitor, built-in video camera, ADSL line, and the latest payment validation technology, the phone is designed to provide what cell phones can't — and to reverse declining use of public phones.

ros — and know which is which — not to mention identify fakes? After all, as of January 1, 2002, pay phones throughout Europe will have to accept euro coins in addition to national currencies, and by March 1 they will have to go on an all-euro diet. The answer, says Ibañez, is a unique feature developed by his team that allows service providers to teleprogram the latest phones for new coins. The provider, whether its Italy's Italtel or Spain's Telfonica, will simply feed the new validation parameters simultaneously into tens of thousands of public phones, which are now being produced at a rate of 500 per day at Elasa. The program can also be used to fine tune the parameters used for accepting existing coins in order to make them even more proficient at recognizing fakes. And what about the so-called "cashless economy"? "Hogwash!" says Ibañez. "We see that where there are phones that offer coin and card payment systems, eighty percent of payments are made with coins." Evidently, money will continue to talk — at least for a few more years.

Arthur F. Pease

Internet Purchasing Power



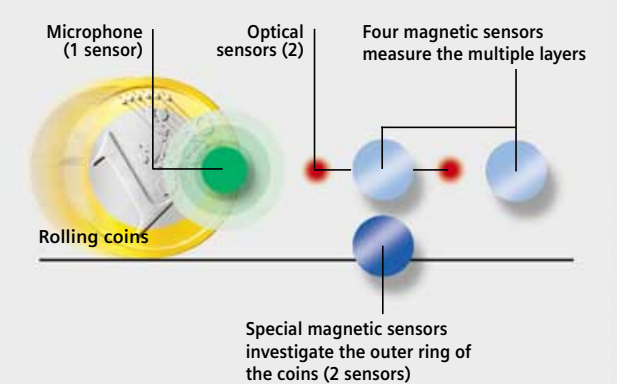
According to a study by Forrester Research, the number of online purchasers in Europe will rise sharply in coming years. By 2004, some two-thirds of Internet users will probably buy goods via the Web — with a PC, cell phone, PDA or TV. On average, they will spend 1,774 euros a year — a powerful argument for developing electronic payment systems.

Inside the New Euro Coins



1- and 2-euro coins will be composed of a refined combination of metals. The bimetallic nature of the outer zone and the center, along with the coin's multilayer structure, makes it easy to definitively identify the coins. This will reduce the chances that fakes will be accepted by vending machines and pay phones.

What Sensors Will See



It will be almost impossible to fool the euro sensors in new vending machines and pay phones. Sensors not only will monitor the sounds coins make, but will also check their optical properties and distinguish the magnetic differences between the edges and centers of the coins.