

First Bank to Launch Electronic Cash

Copyright © 1995 by DigiCash bv.

FOR IMMEDIATE RELEASE (Release Date: October 23, 1995)

Mark Twain Bank of St. Louis Missouri starts accepting applications Monday October 23, 1995 for accounts that can be used to withdraw and deposit ecash over the Internet. DigiCash(TM) bv, of Amsterdam, the Netherlands, developer of ecash, is supplying the technology to Mark Twain Bank under non-exclusive license. The technology has been tested with a 'monopoly(TM) money' currency called CyberBucks(TM), but this U.S. dollar denominated system is the first time electronic cash is actually being offered using real currency.

"This launch marks the beginning of a new era, one in which the digital equivalent of paper money and coins will become even more important than their physical precursors are today," according to Dr. David Chaum, Managing Director of DigiCash bv and inventor of electronic cash. "It will catalyze enormous growth in electronic commerce on the Internet, and prove of enduring value through its improved protection of consumers and society at large."

Sweden Post, another ecash licensee, owns the retail bank that is responsible for more than 50% of value transfers in Sweden and has direct access to accounts of over 75% of Swedish households. Sweden Post has not yet announced its launch date.

How does it work

Using ecash is like using a virtual ATM (Automatic Teller Machine). When connecting to it over the Internet, you authenticate ownership of your account and request the amount of ecash you want to withdraw, much like in person. But instead of putting paper cash in your wallet, your software stores the digital cash it obtains onto the hard disk of your PC.

When you are asked to make a payment on the net, you confirm the amount, purpose and payee and then your ecash software transfers the correct value in coins from your disk. Sellers, ranging from casual participants in the global Internet bazaar to mega-retailers, deposit the digital coins they receive into their accounts.

Behind the user interface, your computer actually chooses the serial numbers of the electronic coins based on a random seed. Then it hides them in special encryption envelopes, provides them to the virtual ATM for signing, and removes the envelopes from what is returned--leaving the bank's validating digital signature on the serial numbers. This way, when the bank receives from the shop the coins you spend, it cannot recognize them as coming from any particular withdrawal, because they were hidden in envelopes during withdrawal. And thus the bank cannot know when or where you shop or what you buy.

The serial number of each signed coin is unique, allowing the bank to be sure it never accepts the same coin twice. In case you wish to identify the recipient of any of your payments, you can also reveal the serial number and prove that you formed it. And, in case your computer were ever to break down, if you had written down the secret random seed number you chose initially when opening your account, future versions would let you use it to re-create the coins in envelopes and thereby obtain a free re-issue of the signed coins that were lost.

How safe is it

Security is fundamental to electronic cash. The cryptographic coding protecting every 5 cent ecash payment is the same as that routinely relied upon for authenticating requests to move huge sums between banks and even for national security. But in principle ecash goes beyond such communications security to achieve true multiparty security: no one (buyer, seller, bank) can cheat anyone else, no matter how they might modify their own software; even if two parties collude, they cannot cheat the third.

Replacing paper and coins with ecash would make life much harder for criminals. Because the payer's computer chooses the serial numbers of the coins, he or she can later irrefutably identify blackmarketeers, extortionists, and acceptors of bribes--were they to take ecash. Paper notes, briefcases full of which can be received without leaving any record, allow money laundering and tax evasion today. With ecash, however, all the amounts each person receives are known to their bank. Significant criminal activity could thus be thwarted by completely replacing paper money; moreover, the privacy of ecash would be essential to widespread acceptance of any electronic payment system that in effect becomes mandatory.

Early, competing, and future systems

Customers of Mark Twain Bank will have to fill out an application form that is available over the Internet, mail or fax it in, and receive a password by mail. The bank's unique multi-currency facilities will allow use from many countries. In the future, the ability to withdraw funds from ordinary checking accounts will be as ubiquitous as making withdrawals at physical ATMs today. Frequent visits to digital branches will give banks the opportunity to offer a full range of financial services to their customers.

The over 60,000 people who registered for the CyberBucks experiment--more than all the other cyber-payment schemes combined--suggests a high level of support and interest in ecash. DigiCash plans to keep the experiment going for those who wish to continue using it.

After CyberBucks went live almost exactly one year ago, and became the first cryptographically protected Internet payment scheme, a plethora of "me-too" schemes have been announced. Most are simply account-based, accepting requests from users to move money from their account to a specified other account, thereby revealing to the central system exactly when, how much, and to whom they pay, and putting users at the mercy of system errors that may result in loss of money or unexpected lock out. Only ecash works with digital coins, empowering people with full control over their side of financial transactions and full control over when and to whom identifying information is released.

Ecash is currently software only: once you've opened an account you just download the software over the net and you're ready to run. DigiCash is developing chip cards and simple readers which will give provide even more security and portability of ecash between machines.

DigiCash does not aim to operate ecash systems itself, but rather to continue developing new versions and licensing to financial institutions.

(The following are trademarks and should always be referred to as such: CyberBucks, DigiCash, ecash, Mark Twain Bank and Monopoly.)

Early Adopter Companies

- AdOne Classified Network (Steve Brotman, +1 212 431 5842, <http://www.adone.com/>)
- BizNet Technologies (Doug Mauer, +1 540 231 7715, <http://www.bnt.com/>)
- Consensus Development Corporation (Christopher Allen, +1 510 559 1500, <http://www.consensus.com/>)
- Delorie Software (<http://www.delorie.com/>)
- Global-X-Change Communications (Elliot Burdett, +1 613 235 6865, <http://www.globalx.net/>)
- PULVER.COM (Jeff Pulver, +1 917 336 8240, <http://www.pulver.com/>)
- Sun Microsystems (Humphrey Polanen, +1 415 336 0022, <http://www.sun.com/>)
- The Electronic Frontier Foundation (EFF) (Stanton McCandlish, +1 415 668 7171, <http://www.eff.org/>)
- The Electronic Privacy Information Center (EPIC) (Marc Rotenberg, +1 202 546 6520, <http://www.epic.org/>)
- The New Sun Newspaper (Lese Dunton, +1 212 799 7402, <http://shebute.com/newsun/today/>)
- The Well (Bruce Katz, +1 415 332 4335, <http://www.well.com/>)
- Walter Shelby Group (John Buckman, <http://www.shelby.com/pub/shelby/>)

These companies offering their clients ecash

- Husky Labs (David Levine, +1 410 889 3409, <http://www.butterfly.net/>)
(Clients: National Public Radio, The National Geographic Society, PoliticsUSA, Penguin Books, E-Z Communications, Pentagon Cds and Tapes, AfroAmerican Newspapers, Ellicott Machine Corp., The Greater Baltimore Committee Technology Council, National Petroleum Council, Netv, Review.Net, Robert Rytter & Associates, and United States Holocaust Memorial Museum)
- Organic Online (Brian Behlendorf, +1 415 284 6888, <http://www.organic.com/>)
(Clients: Advertising Age, Saturn Cars, Rubin Postaer Agency, Sybase, Inc., Volvo Cars of North America, Xircom, 1-800-Collect, Conari Press Books, Great Americian Music Hall, City of Tribes Communications, Octel, Montgomery Securities, Macromedia)
- Poppe Tyson Advertising (Fergus O'Daly, +1 212 727 5600, <http://www.poppe.com/>)
(Clients: American Express Travel Agency, PSINet Inc., Intercon Systems Corp., Fordham University, New York Cruise Lines Inc., Osram Sylvania, Pfizer, Food Service Group, Ridgewood Savings Bank, Warner Lambert, Drew, EUA COGENEX, New Jersey Travel and Tourism, AT&T, American Isuzu Motors, DataProducts, Magellan, Toshiba America, Computer Systems Division, Toshiba Computer Systems, Toshiba Disk Products, Applied Medical Informatics, Cascade Design Automation, Chrysler Corp. Cirrus Logic, Cypress Semiconductor, Escalade, Hewlett-Packard, Hyundai Electronics America, Intel Corp., International Network Services, Internet Profiles Corp., LANNET, Logic Modeling, Measurex, MIPS Technologies, Netscape Communications Corporation, Network Equipment Technologies, Network General, Nokia, North Mountain Software, Premisys Radiomail, Red Herring Magazine, Robert Half International, Sony Electronics Inc., Broadcast Product Group, Sync Research, Synopsys, Synopsys Logic Modeling Group, Touche, Valvoline)

Back to the [press releases page](#).