

Date: Tue, 7 May 1996 00:25:44 +0200
From: press@digicash.com
To: ecash@digicash.com
Subject: Press Release: Ecash to be Issued by Deutsche Bank
Sender: owner-ecash@digicash.com
Precedence: bulk

Please find attached today's press release on our cooperation with Deutsche Bank. If you need any further information, please contact us at: press@digicash.com

Kindest regards,

Paul Dinnissen
DigiCash BV

----- PRESS RELEASE -----

Release date:
Tuesday, May 7, 1996
Amsterdam, The Netherlands

=====
DigiCash's Ecash to be Issued by Deutsche Bank
=====

DigiCash and Deutsche Bank are to launch a joint pilot project to test the use of electronic cash on the Internet. This will enable Deutsche Bank's clients to pay for information (ranging from magazine articles to stock quotes), services (from database searches to help desk support) and tangible goods (from mail order to pizzas) using any personal computer with access to the Internet. This new service will provide merchants and even private individuals with the solutions needed for doing business on the Internet.

The project's technology is based on the ecash system, which won DigiCash the European Commission's 1995 Information Technology European Award (ITEA'95) for innovative technology. Ecash has been tested for several years and was used last autumn to issue the first ecash dollars in the USA.

Apart from a PC, users do not need any special hardware or cards. They simply connect to Deutsche Bank's Internet site and download digital ecash coins onto their PC's hard disk, thereby debiting their accounts. These coins can later be used as needed to pay on the Internet withby a single mouse-click.

"In launching this pilot project, Deutsche Bank aims to test the possibilities of innovative payment forms and procedures and to expand their range of Internet services" says Dr. Wolfgang Johannsen, Head of Deutsche Bank's Department for Technological Development.

"Ecash is a digital form of cash that works on the Internet where paper cash can't" according to Dr. David Chaum, founder and CEO of DigiCash. "Like cash, it offers consumers true privacy in what they buy. Yet, users can always recover their money if their computer crashes, and also prove who received their electronic cash in payment, making it unsuitable for criminal use. Thus ecash brings an improved form of cash to cyberspace, where it can be expected to

catalyze an enormous growth in electronic commerce."

DigiCash and Deutsche Bank see this launch as a major step towards the adoption of true electronic cash on the Internet.

Contact DigiCash Amsterdam:

Mr. Paul Dinnissen

Tel: +31 20 665 2611

Fax: +31 20 665 1126

email: press@digicash.com

<http://www.digicash.com/>

Contact Deutsche Bank:

Mr. Schumacher / Mr. Thoma

Tel: +49 69 910 33406 / 33405

Fax: +49 69 910 33422 / 38689

<http://www.deutsche-bank.de/>

(DigiCash and ecash are registered trademarks
and should always be referred to as such)

* * *

DigiCash Backgrounder

=====

History and Mission

Since beginning operation in April 1990, DigiCash's mission and primary activity has been: to develop and license payment technology products--chip card, software only, and hybrid--that both show the true capability of technology to protect the interests of all participants and are competitive in the market.

Founder

Dr. David Chaum, managing director of DigiCash, received his Ph.D. in Computer Science from the University of California at Berkeley, then taught at New York University Graduate School of Business Administration and at the University of California, and headed the Cryptography Group at CWI, the Dutch nationally funded center for research in mathematics and computer science, before taking his current position. He has published over 45 original technical articles on cryptography and also founded the International Association for Cryptologic Research.

DigiCash Products

Blue: smart card technology for EMV & prepaid with dynamic public key. Conforms to joint Europay, MasterCard, Visa specifications; multiple applications, including loyalty and closed systems; superior data integrity in case of malicious/accidental interference or interruption; requires only the smallest and most proven chips, e.g. SC-24 or ST601; mask technology licensing.

CAFE: smart card and card-accepting electronic wallet project. Consortium of 12 other members founded and chaired by Dr. Chaum of DigiCash; simulation, mask and first readers developed by DigiCash; technology trial at the EC headquarters building in participation with related open special interest group and partially funded by the EC.

DyniCash: highway-speed road-toll collection system using smart cards. Chip card inserts into battery-powered dashboard unit; reflective backscatter microwave technology by industry leader Amtech; prepaid mode has user privacy; open and/or closed pricing schemes; tested extensively in Japan; non-exclusive licensing of the payment technology.

Ecash: software only electronic cash system for internet/email. Users download software that can make and receive payments; protects users' money like travellers checks and privacy like coins; now operational after testing by over twenty thousand users world-wide; Macintosh, MS-Windows and X-Windows; any WWW browser; currently Mark Twain Bank currently issues ecash in US dollars and Mearita/EUnet issues digital Finnish marks; Posten has announced their license and intention to issue Swedish Kroner.

Facility Card: complete facility management smart-card/reader system. Cash replacement, access control, and time/attendance system; now in schools, hospitals, industry, offices, recreation; interfaces to vending, point-of-sale, access control, copiers, phones, gaming; downloadable & upgradeable readers work on-line and/or off-line; sold through VAR's; over 100k cards in use in the Netherlands; Mars Electronics International will launch it globally in 1996.

Ecash Backgrounder

=====

How does ecash work?

Using ecash is likeas easy as using a virtual ATM (Automatic Teller Machine). When you connect over the Internet and authenticate your ownership of the account, you can withdraw money electronically. Instead of giving you bank notes, you are given digital coins which your software can store on your PC's hard disk.

When you want to make a payment, you simply confirm the amount, payee and description of goods, with a mouse click you tell your ecash software to transfer coins of the correct value from your PC direct to the payee. Merchants, (ranging from casual participants in the global Internet bazaar to mega-retailers) can then deposit the digital coins into their ecash accounts.

Behind the user interface, your computer actually creates 'serial' numbers for the electronic coins based on a random 'seed'. Then it hides them in special encryption 'envelopes', sends them to the electronic bank for 'signature' and, when they are returned, removes the 'envelopes' (retaining the bank's validating digital signature on the 'serial' numbers). This way, when the bank (eventually) receives your coins, it cannot recognize them as coming from any particular withdrawal or account, because all coins are hidden from the bank during the withdrawal process. Therefore the bank cannot know when or where you shop, who you pay or what you buy.

The 'serial' number' of each signed coin is unique, so that the bank can be sure that it never accepts the same coin twice. If you wish to identify the recipient of any of your payments, you may reveal the unique coin number and use your ecash software to prove

that you created it and get the bank to confirm who deposited it. Your software can also re-create the `serial' numbers and `envelopes' from the `seed' that you wrote down when installing your account, thereby allowing all your coins to be re-created if your PC fails.

How safe is ecash?

Security is fundamental to electronic cash. The cryptographic coding that protects 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 (as mentioned above), he or she can later irrefutably identify blackmarketeers, extortionists, and acceptors of bribes--were they to accept ecash. Paper notes, briefcases full of which can be passed from hand to hand 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 whichof ecash offers would be essential to widespread acceptance of any electronic payment system.

----- END PRESS RELEASE -----