News from CAFE — The High Security Digital Payment System —

Matthias Schunter
Universität Hildesheim
schunter@informatik.uni-hildesheim.de

Arnd Weber
Institut für Sozialforschung, Frankfurt
100136.2063@CompuServe.com

June 12th, 1995

CAFE ("Conditional Access for Europe") is a project sponsored by the European Union. It has designed the most advanced multiparty-secure secure payment system so far, which is now trialed at the EU premises in Brussels. It started in Dec. 1992 and ends in Nov. 1995.

The consortium consists of groups for social and market studies: Cardware (GB), Institut für Sozialforschung (D); software and hardware producers: DigiCash (NL), Gemplus (F), Ingenico (F), Siemens (D); and designers of secure cryptographic protocols: CWI (NL), PTT Research (NL), SEPT (F), Sintef Delab Trondheim (N), Universities of Aarhus (DK), Hildesheim (D), and Leuven (B).

An important aspect of CAFE is high security of all parties concerned, with the least possible requirements that they are forced to trust other parties (multi-party security), and less dependence on the tamper-resistance of devices than with other proposals for stored value cards. CAFE proposes an open architecture for small and high value payments, post-pay (like credit cards) or pre-pay (like stored value cards). For small everyday transactions all payments can be made offline, and privacy is an important issue. Other features are

- loss tolerance,
- different currencies,
- and an open architecture.

The basic techniques used in the CAFE protocols have been sketched in [BBCM94].

Since then, the site for the field trial has been fixed to be on the premises of the European Union. The trial will be operable in June 1995. It already uses hardware designed for mass production.

The European Union is a good place for developing advanced payment systems, since development is not hampered by export restrictions for cryptologic primitives (except for France).

The devices used in CAFE are so-called electronic wallets. Two types will be trialed, a simple one with just two buttons and a display and one with more buttons. Advantages of buttons are that PINs can be entered directly, so that fake-terminal attacks are prevented or that certain amounts may be unlocked beforehand to prevent the observation of PIN entry. According to the surveys, enough customers are willing to pay the price of these devices (up to $60), although a large share require them to be very thin to fit in a regular wallet. The protocols could also be run in multi-functional devices like PDAs or mobile phones. The wallets in the trial use smartcards as money storage. In the trial, it is currently possible to use the smartcards without the wallets, too, although this reduces the amount of control the user has over his money. The system could also be used for network payments (electronic marketplaces). Since the wallets simply communicate via infrared, the disadvantages of needing special hardware and connecting them may well be outweighed by the advantages: The consumer's money is not handled in an unprotected general-purpose computer (the consumers appreciated the idea to keep their wallet always in their hand), and the same system can be used for network and other payments.

A "Special Interest Group Multicurrency Electronic Wallets" (SIGMEW) related to this trial has been formed with support of the European Union; about 30 organizations, in particular financial ones, have joined (e.g., Abbey National, Allied Irish Bank, Bank Axept, Barclays, Cartes Bancaires, Deutsche Bank, Europay, Mastercard, Sligos, Visa). The SIGMEW is chaired by Mr. Willie O'Reilly, General Manager Development, Allied Irish Bank, Dublin (Phone +353 1 6600311, Fax +353 1 6604945). It shall continue after the end of the CAFE project.

For more details, see [BBCM94] or the CAFE simulation [CAFE94], or contact our project manager, Ray Hirschfeld (ray@cwi.nl). For the SIGMEW, contact Chris Stanford or Bob Carter, Cardware, (100116.424@compuserve.com).

References

[BBCM94] Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen, Stig Mjølsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallée, Michael Waidner: The ESPRIT Project CAFE - High Security Digital Payment Systems; ESORICS 94 (Third European Symposium on Research in Computer Security), Brighton, LNCS 875, Springer-Verlag, Berlin 1994, 217-230.

Abstract and paper:

`http://www.informatik.uni-hildesheim.de/~sirene/lit/abstr94.html`

[CAFE94] CAFE simulation; http://www.digicash.com /cafe/download.html (requires MS Windows).