# CAFE — Ein sicheres datenschutzorientiertes Zahlungssystem

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

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

CAFE („Conditional Access for Europe") entwickelte im Rahmen des Forschungsprogramms ESPRIT der Europäischen Union ein sicheres anonymes Zahlungssystem. Es ist bei bei Offline-Zahlungen weltweit technologisch führend. Anfang Juli '95 startet ein Feldversuch bei der Europäischen Union in Brüssel. Hierbei werden Karten und taschenrechnerartige elektronische Geldbörsen verwendet.

Das Konsortium besteht aus

- Sozial- und Marktforschungsinstitutionen: Cardware (GB), Institut für Sozialforschung (D);
- Soft- und Hardwareentwicklern: DigiCash (NL), Gemplus (F), Ingenico (F), Siemens (D);
- und einer Gruppe für die Entwicklung der sicheren kryptografischen Protokolle: CWI (NL), PTT Research (NL), SEPT (F), Sintef Delab Trondheim (N) und die Universitäten Aarhus (DK), Hildesheim (D) und Leuven (B).

CAFE entwickelte eine offene Sicherheitsarchitektur für beliebige Zahlungen. Anwendungsbeispiele sind Wertkarten, wie z.B. Telefonkarten, oder Kreditkarten. Kleinere Zahlungen können hierbei ohne Interaktion mit der Bank erfolgen (Offsline). Hauptziel von CAFE war, einen hohen Grad an Sicherheit für alle beteiligten Parteien zu bieten, wobei im Idealfall jede Person ihre Sicherheit selbst kontrollieren und erzwingen kann (z.B. hängt der Datenschutz der Kunden nicht von der Verschwiegenheit der Bank ab: Sie erhält keine überflüssigen Daten und kann somit auch keine Daten weitergeben). Außerdem wurde versucht, möglichst geringe Anforderungen an die Manipulationssicherheit der Geräte (z.B. Chipkarten) zu stellen.

Das System sich durch folgende Eigenschaften aus:

- Verlusttoleranz (bei Verlust der Karte kann der enthaltene nichtverbrauchte Geldbetrag bestimmt und erstattet werden),
- mehrere Währungen durch mehrere „Währungsfächer" und
- eine offene Sicherheitsarchitektur (geeignet für mehrere Banken, Händler und Kunden, die sich gegenseitig nicht vertrauen müssen).

Die in CAFE verwendeten Geräte sind sogenannte elektronische Brieftaschen (electronic wallets) mit Datenübertragung per Infrarot. Im Versuch werden eine einfache Ausführung mit „JA“- und „NEIN“-Tasten zur Bestätigung von Zahlungen und eine leistungsfähigere Variante mit numerischer Tastatur zur Eingabe von Geheimzahlen (PIN) erprobt. Die numerische Tastatur im Gerät erschwert das Abfangen oder Ablesen der Geheimzahl. Laut Verbraucherumfragen ist hierfür auch ein Markt vorhanden: Viele Verbraucher würden die Kosten (bis zu 100DM) bezahlen, insbesondere, wenn die kleinen Geräte auch weitere Funktionalität, wie Termin- oder Adreßverwaltung bieten. Außerdem begrüßten sie die Idee, die eigenen Geräte nie aus der Hand zu geben. Die entwickelten Protokolle könnten jedoch ebensogut auf größeren Geräten, wie PDAs oder Mobiltelefonen implementiert werden. Für den Feldversuch werden teilweise auch reine Chipkarten verwendet, obwohl dies die Sicherheit der Benutzer stark einschränkt, da eine geschützte Benutzerschnittstelle fehlt. Da keine Annahmen über die Datenübertragung zwischen den Geräten gemacht wurden, eignet sich das System ebenso für Zahlungen über unsichere Netzwerke (z.B. Internet).

Für die Unterstützung des Projekts, des Feldversuchs in Brüssel und der Verwertung der Ergebnisse wurde eine “Special Interest Group Multicurrency Electronic Wallets” (SIGMEW) mit Unterstützung der EU gegründet. Derzeit hat die Gruppe ungefähr 30 Mitglieder. Diese stammen vorwiegend aus dem Finanzsektor (z.B. Abbey National, Allied Irish Bank, Bank Axept, Barclays, Cartes Bancaires, Deutsche Bank, Europay, Mastercard, Sligos, Visa). Vorsitzender der SIGMEW ist Mr. Willie O’Reilly, General Manager Development, Allied Irish Bank, Dublin (Phone +353 1 6600311, Fax +353 1 6604945).

Als weiterführende Information dienen [Chau92] (allgemeinverständliche Beschreibung der Grundlagen anonymer Zahlungssysteme), [BBCM94] (mehr über die CAFE Protokolle) oder [CAFE94] (CAFE-Demoprogramm).

Weitere Informationen zu CAFE bieten Ray Hirschfeld (ray@cwi.nl) oder die Autoren, zur SIGMEW der Vorsitzende der SIGMEW oder Chris Stanford und Bob Carter von Cardware (100116.424@compuserve.com).

## Literatur


[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).

[Chau92] David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.