

Series Editor-in-Chief **Saba Zamir**
CRC PRESS Advanced and Emerging
Communications Technologies **SERIES**

S E C O N D E D I T I O N

Protocols for Secure Electronic Commerce

Mostafa Hashem Sherif

 **CRC PRESS**

S E C O N D E D I T I O N

Protocols for Secure Electronic Commerce

Mostafa Hashem Sherif, Ph.D.

AT&T Laboratories, New Jersey

Series Editor-in-Chief

Saba Zamir



CRC PRESS

Boca Raton London New York Washington, D.C.

IPR2023-00744

Fintiv Ex. 2010 | Page 2 of 4

Library of Congress Cataloging-in-Publication Data

Sherif, Mostafa Hashem.

[Monnaie électronique. English]

Protocols for secure electronic commerce / Mostafa Hashem Sherif. — 2nd ed.

p. cm. (The CRC Press advanced and emerging technologies series)

Includes bibliographical references and index.

ISBN 0-8493-1509-3 (alk. paper)

1. Electronic commerce. 2. Bank credit cards. 3. Computer networks—Security measures. I. Title. II. Series.

HF5548.32.S5213 2003

658.8'72'028558—dc22

2003061098

This book contains information obtained from authentic and highly regarded sources. Reprinted material is quoted with permission, and sources are indicated. A wide variety of references are listed. Reasonable efforts have been made to publish reliable data and information, but the author and the publisher cannot assume responsibility for the validity of all materials or for the consequences of their use.

Neither this book nor any part may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, microfilming, and recording, or by any information storage or retrieval system, without prior permission in writing from the publisher.

The consent of CRC Press LLC does not extend to copying for general distribution, for promotion, for creating new works, or for resale. Specific permission must be obtained in writing from CRC Press LLC for such copying.

Direct all inquiries to CRC Press LLC, 2000 N.W. Corporate Blvd., Boca Raton, Florida 33431.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation, without intent to infringe.

Visit the CRC Press Web site at www.crcpress.com

© 2004 by CRC Press LLC

No claim to original U.S. Government works

International Standard Book Number 0-8493-1509-3

Library of Congress Card Number 2003061098

Printed in the United States of America 1 2 3 4 5 6 7 8 9 0

Printed on acid-free paper

by the central bank) and to the traceability of the transactions and the movement of money.

The units of payment contained in the cards or in the software are bought either with fiduciary money or by charging to a bank account. The discharging power of these units is restricted to those merchants who accept them. This is the reason certain experts consider that electronic money does not exist in a strict sense, because it is neither legal tender nor does it have discharging power (Fay, 1997, p. 113).

2.3.2 Virtual Money

Virtual money differs from electronic money in that its support, its representation, and its mode of payment do not take tangible forms. Virtual money can be contained in software programs that allow payments to be carried out on open networks, such as the Internet.

Starting with the definition of the BIS for electronic money, one can consider virtual money as a referent (or a pointer) to a bank account. The scriptural character of the virtual money is also tied to the status of the issuer (it is not issued by the central bank) and to the traceability of the transactions.

In the limiting case, virtual money may also be a virtual token (or *jeton*) issued by a trusted issuer for unique usage in a closed circuit.¹ These jetons are different from the electronic versions of legal tenders because they are recognized only in a restricted commercial circuit. This contrasts with electronic money, which is a multipurpose payment mechanism recognized in general commercial circuits. Millicent, for example, is one system that proposes a method for micropayments with a virtual jeton, the “scrip.” A service provider issues a scrip, which does not have any direct relationship with the banking system but is a promise for future service. By generalizing this notion, service providers can issue their jetons and tie them with banking accounts that they maintain. They will remain within the perimeter defined by the law as long as these units are ascribed to a specific purchase within a well-defined circuit.

Telephone cards are a particular case of virtual purses issued by telephone companies. These cards are prepaid, and the values they store are dedicated to the settlement of telephone communications at a given service provider. The purchasing power is described in terms of “telephone jetons” that correspond to the impulse counts in the telephone networks. The experiences of the telephone card and of the Minitel kiosk show that, when the amounts under consideration are individually marginal, a telephone operator, although a “nonbank,” can effectively help in collecting amounts that are

¹The dictionary (Webster's New Collegiate Dictionary, 1975) definition of token is “a piece resembling a coin issued as money by some person or a body other than a de jure government.” Despite this clear statement, there has been a tendency to mix legal coins with tokens (see, for example, Camp et al., 1995). To avoid the potential confusion, this book will use the French word *jeton* to mean a coin issued by a nongovernmental body.