American National Standard
for Financial Services

X9.49 -1998

Secure Remote Access to Financial Services For the Financial Industry

Secretariat:
Accredited Standards Committee X9, Inc.

Approved: November 9, 1998

American National Standards Institute

American National Standard

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by:

Accredited Standards Committee X9, Inc.
P.O. Box 4035
Annapolis, Maryland 21403 USA
Phone: 410-267-7707 or 301-879-7988
Fax: 301-879-5124
Email: Cindy.Fuller@X9.org
Isabel.Bailey@X9.org
X9 Online: http://www.x9.org

CONTENTS

TABLES

FIGURES

FOREWORD

(This Foreword is included for information only and is not part of this Standard)

Business practice has changed with the introduction of computer-based technologies. The substitution of electronic transactions for their paper-based predecessors has reduced costs and improved efficiency. Trillions of dollars in funds and securities are transferred daily by telephone, wire services, and other electronic communication mechanisms. The high value or sheer volume of such transactions within an open environment exposes the financial community and its customers to potentially severe risks from accidental or deliberate alteration, substitution or destruction of data. This risk is compounded by interconnected networks and the increased number and sophistication of malicious adversaries.

Some of the conventional "due diligence" controls used with paper-based transactions are unavailable in electronic transactions. Examples of such controls are safety paper which protects integrity, and handwritten signatures or embossed seals which indicate the intent or the originator to be legally bound. In an electronic-based environment, controls must be in place that provide the same degree of assurance and certainty as in a paper environment.

In order to maintain the appropriate access security for financial systems, means are required to provide the authorized user with credentials which reliably identify the user to the protected system or application. Having established an authenticated identity, it is then necessary to provide the means for the user to securely pursue his/her legitimate business session with the protected system and applications.

The effectiveness of the security afforded by the credentials employed in the identity authentication procedure, however, is dependent upon each user having credentials that are user unique and which are highly resistant to counterfeit.

The effectiveness of the security afforded by the session security measures are dependent upon the specific security services invoked for that purpose.

The process whereby specific security services are selected and configured for purposes of user authentication and session security is the subject of this Standard.

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to Accredited Standards Committee X9, Inc., P.O. Box 4035, Annapolis, Maryland, 21403 USA.

This Standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval. At the time that this Standard was approved, the X9 Committee had the following members:

Harold Deal, X9 Chair
Bill Lyons, X9Vice Chair
Cynthia Fuller, Managing Director
Darlene Schubert, Program Manager

Organization Represented	Representative
American Bankers Association	Anne Livingston
	Kawika Daguio
American Express Company	Bonnie Howard
	Jill Mars
Applied Communications Inc.	Doug Grote
	Cindy Rink
AT&T	Steve Lind
Automated Financial Services	Thomas Clute
Banc One Services Corporation	Bil Lyons
Bank of America	Harold Deal
	Gretchen Breiling
Bankers Roundtable	Fred Honold
	Keviar Warner
Canadian Bankers Association	Christine Arjoonlal
	Mara Bakic
Certicom Corporation	Don Johnson
Chase Manhattan Bank	Francis Keenan
	Christopher Dowdell
Citibank	Seymour Rosen
Cybersafe Corporation	Glenda Barnes
	David O'Brien
DataCard Corporation	Charles Baggeroer
	Dirk Helgemo
Deluxe Corporation	Maury Jansen
Discover Card Services Inc.	William Kabat
Ernst & Young, LLP	Geoffrey Turner
	Rick Kastner
	Ralph Poore
Federal Reserve Bank	Dexter Holt
	Susan Belisle
	Gary Chaulklin
	Jean Lovati
Ferris & Associates	Martin Ferris
First Data Corporation	Gene Kathol
IBM Corporation	Harry Hankla
	Don Harman
Intel Corporation	Steve Ellis
	Pamela Warren
KPMG Peat Marwick LLP	Jeff Stapleton
M. Blake Greenlee Associates, Ltd.	Blake Greenlee
MARS Electronic International	E. E. Barnes
	Ron Bernardini
MasterCard International	Melinda B. Yee
	Ron Karlin
Mellon Bank, N.A.	David Taddeo

	Genien Carlson
Merrill Lynch	John Dolan
Moore Business Forms, Inc.	Thomas Oswald
National Association of Convenience Stores	Robert Swanson
National Security Agency	Jerry Rainville
NCR	Steve Stevens
New York Clearing House	Vincent DeSantis
NOVUS Services, Inc.	Thomas Kossler
	Peggy Douds
	David Pratscher
Pitney Bowes, Inc.	Leon Pintsov
PricewaterhouseCoopers	Jeff Zimmerman
SPYRUS	Peter Yee
	Karen Randall
Unisys Corporation	Tom Hayosh
	James Graziano
VeriFone, Inc.	John Sheets
	Brad McGuinness
	Trong Nguyen
	Stuart Taylor
VISA International	Bill Chen
Wells Fargo Bank	Tim Silva
Xcert International, Inc.	Marc Branchaud
	Sandra Lambert

The X9F subcommittee on Data and Information Security had the following members:

Glenda Barnes, Chair	Cybersafe Corp.
Sandra Lambert, Vice Chair	Xcert International, Inc.
Organization Represented	**Representative**
American Bankers Association	Kawika Daguio
American Express Company	Bonnie Howard
	Glen Weiner
Applied Communications Inc.	Cindy Rink
	Douglas Grote
Bank of America	Mack Hicks
	Kathleen Gibbons
	Richard Phillips
	Martin Johnson
Bank One Corp.	Duane Baldwin
Bankers Roundtable	Keviar Warner
	Frederick Honold
Certco LLC	Richard Ankey
	Daniel Geer
Certicom Corporation	Donald Johnson
Chase Manhattan Bank	Gene Rao

	Richard Yen
Communication Security Establishment	Alan Poplove
	Michael Chawrun
Cybersafe Corporation	Glenda Barnes
	David O'Brien
Cylink Corporation	Kamy Kavianian
	Lily Lidong Chen
Deluxe Corporation	Cory A. Surges
	Maury Jansen
	Chuck Bram
Diebold, Inc	Sandy Morgan
	Roy Shirah
Digital Equipment Corporation	Donald Holden
Entrust Technologies	Robert Zuccherato
	Tim Moses
Ernst & Young, LLP	Richard Kastner
	Ralph Spencer Poore
Federal Reserve Bank	Richard Sweeney
	Michael Versace
	Gary Chaulklin
First Data Corporation	Gene Kathol
First Union Corporation	James Ramsey
	Sandra Lambert
Fortress Technologies	Eva Bozoki
Gilbarco, Inc.	Rena Smith
Griffin Consulting	Phillip Griffin
	Harriette Griffin
GTE Internetworking	Patrick Cain
Harmonic Systems, Inc.	Daniel Hunt
IBM Corporation	Mohammad Peyravian
	Harry Hankla
	Stephen Mike Matyas
IIT Research Institute	Roger Westman
Intel Corporation	Tom Jones
KPMG Peat Marwick LLP	Jeffrey Stapleton
M. Blake Greenlee Associates. Ltd.	Blake Greenlee
MasterCard International	Ron Karlin
	William Poletti
Mellon Bank, N.A.	David Taddeo
Merrill Lynch	Lawrence LaBella
	John Dolan
	Ted Gerbracht
National Association of Convenience Stores	Robert Swanson
National Security Agency	Gerard Rainville
NCR	Mark Liddle
NIST	Donna Dodson
	Miles Smid

Northern Telecom, Incorporated	Warwick Ford
Northstar Technology Group, Inc.	John Bowman
Pitney Bowes, Inc.	Andrei Obrea
PricewaterhouseCoopers	John D. Hunt
	David Oshman
	Jeffrey Zimmerman
Pulse EFT Association	Karen Gardstein
	Leslie Handrix
Racal Guardata, Inc.	Scott Petersen
	Emile Soueid
	Samuel Epstein
SAIC	Wanda Gamble-Braggs
Security Dynamics	Burt Kaliski
SPYRUS	Karen Randall
	Peter Yee
Technical Communications Corporation	John Gill
TECSEC Incorporated	Edward Scheidt
	Jay Wack
US Department of Treasury	Gary Grippo
VeriFone, Inc	John Sheets
	Stuart Taylor
	Trong Nguyen
VISA International	William Chen
Wells Fargo Bank	Azita Amini
	Terry Leahy
Xcert International, Inc.	Marcus Branchaud

The X9F4 Working Group which developed this Standard had the following members:

George Soerheide, Chairman	Security Dynamics, Inc.

Representative	Organization Represented
Dennis “Abe” Abraham	Abraham & Associates
Azita Amini	Wells Fargo Bank
Todd Arnold	IBM
Glenda Barnes	Sagus
David Black	Sage Technology
Mauro DeFelice	Mellon Bank
Jim Dray	NIST
Jamie Edelkind	Sage Technology, Inc.
Lore Eisenstaedt	Advantis
Roger Fischer	Norwest Technical Serv.
Jim Foti	NIST
Kathleen Gibbons	Bank of America
Sally Graham	Bank of America
Tom Jones	Intel
Rick Kastner	Ernst & Young

Kamy Kavianian	CYLINK
Shirley Kawamoto	MITRE Corp.
George Lundrigan	Wayne/Dresser
Debra O'Dell	Lockheed Martin
Rup Parmar	VanCity Savings CU
Bill Poletti	MasterCard International
Lisa Pretty	Certicom
John Pratt	EXXON
Karen Randall	Spyrus
Pud Reaver	National Security Agency (NSA)
Jeff Stapleton	Security Dynamics
Linda Taylor	Bank of America
Henry Tsui	First Data Corp.
Jennifer Vancini	Certicom
Michael Versace	Federal Reserve, Boston

1. Introduction

1.1 Scope

This standard provides for the secure remote access to and exchange of financial information/data between users and financial service providers.

This standard is used to develop a security approach for remote access to financial services and exchange of financial data by examining the threats, vulnerabilities, and resulting risks to the data elements, transactions, and operational features of a financial service.

This standard specifies a minimum set of security safeguards for financial data used in this manner. Financial service providers and remote access are defined in Section 2, *Definitions and Common Abbreviations*.

Once a user has been authenticated by a financial service provider, access rights are assigned according to the policies of that provider. The assigning of access rights is beyond the scope of this standard.

This Standard is platform/device independent and uses existing standards as appropriate. The physical security of the financial system, although important, is beyond the scope of this standard. Refer to *ANSI X9-TG-5 Information Security Guidelines*.

1.2 Purpose

The purpose of this standard is to define the minimum security requirements for a secure and protected exchange of information between a user and a financial service provider. The standard is intended for use by banks and other payment system intermediaries (e.g. technology and service providers) to implement controls that reduce the operational risks in remote access-based financial systems. The protection offered will:

- provide integrity for a message during transmission
- provide for secrecy of the message during transmission
- identify the rightful user and financial service provider prior to and during data transmission
- prevent repudiation of a message or transaction by either party.

The level of protection employed in a financial service's electronic data access network will depend directly on the sensitivity of the information being exchanged, and thus could vary from application to application.

1.3 How to use this document