

ANS

X9.49-1998

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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>**

Copyright © 1998 by Accredited Standards Committee X9, Inc.
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher.
Printed in the United States of America

CONTENTS

Foreward	i
American National Standards Institute	i
1. Introduction	1
1.1 Scope	1
1.2 Purpose	1
1.3 How to use this document	1
2. Definitions and Common Abbreviations	3
2.1 Definitions	3
2.2 ANSI References	5
2.3 US Government References	6
2.4 ISO References	7
3. Risk Analysis	7
3.1 Introduction	7
3.2 Risk Level Analysis	8
3.3 Environmental Considerations in the Risk Assessment	9
3.4 Cryptographic Considerations in the Risk Assessment	11
3.5 Optional Modifications	11
3.6 Alternate Risk Assessment Methodologies	12
4. Data Confidentiality	12
4.1 Introduction	12
4.2 Confidentiality Risk Analysis	13
4.3 Minimum Security Requirements for Confidentiality	14
5. Integrity	15
5.1 Introduction	15
5.2 Integrity Check Value	15
5.3 Integrity Check Value Schemes	15
5.4 MAC for Data Integrity	16
5.5 Digital Signature for Data Integrity	16
5.6 Data Integrity Risk Analysis	17
5.7 Security Requirements for Integrity	19
6. IDENTITY AUTHENTICATION	19
6.1 Introduction	19
6.2 Authentication Model	19
6.3 Credentials and Identity Factors	20
6.4 Identity Authentication Process	21
6.4.1 The Authentication Process	21
6.4.2 Basic Attributes of Credentials	22
6.4.3 Entity Authentication via Credentials	22
6.5 Options for Identity Authentication	23
6.6 Entity Access Control	23

6.7	Credentials And Identity Factor Characteristics	23
6.7.1	Knowledge Credentials	23
6.7.2	Knowledge Factor	24
6.7.3	Minimum Authentication Criteria	24
6.7.4	Possession Credentials	25
6.7.5	Possession Identity Factor	25
6.7.6	Minimum Authentication Criteria	26
6.7.7	Biometric Credentials	26
6.7.8	Biometric Identity Factor	27
6.7.9	Minimum Authentication Criteria	27
6.8	Authentication Risk Analysis	27
6.8.1	Risk Questionnaires	27
6.8.2	Minimum Security Requirements	29
6.9	Credentials Management	29
6.9.1	Credential Life Cycle	29
6.9.2	Policies and Procedures	29
7.	Message Non-repudiation and Proof of Origin	33
7.1	Introduction	33
7.1.1	Rationale for Cryptographic Non-Repudiation	33
7.1.2	The Generation of Digital Signatures	33
7.1.3	Certification of Keys	33
7.2	Repudiation Risk Analysis	34
7.3	Security Requirements for Non-Repudiation	35
8.	Key Management	36
9.	Security of Remote Financial Service Data and Processes	38
9.1	Financial Service Security Responsibilities	39
9.2	User Authentication to the Remote Access Device	39
9.3	Data Confidentiality on the Remote Access Device	39
9.4	Data Integrity on the Remote Access Device	39
Annex A:	Risk Analysis	41
A.1	Introduction	41
A.2	System Risk Assessment	41
A.3	Business Risk Questionnaire	44
A.4	Risk Assessment	45
Annex B:	Relevant ANSI Standards	53
Annex C:	Synchronous Key Techniques	59
Annex D:	Authentication Schemes	63
Annex E:	Security Considerations	65
E.1	Cryptographic Hardware	65
E.2	Environmental Vulnerability	67

Annex F: Risk Assessment Examples	70
F.1 Game Scenario	70
F.1.2 Transactions	72
F.2 Risk Assessment	75
F.3 Security Requirements	79
Annex G: Registration Process	81
G.1 Credential Application	82
G.2 Credential Validation	83
G.3 Service Preparation and Notification	83
G.4 Service Verification	84

TABLES

Table 1 Data Confidentiality Requirements	13
Table 2 Data Integrity Requirements	18
Table 3 Credential and Identity Factor Examples	21
Table 4 Authentication Security Requirements.....	28
Table 5 Non-Repudiation Requirements	35
Table A 1 Risk Assessment Model.....	41
Table A 2 Security Requirements Matrix	52
Table E 1 Cryptographic Hardware Considerations	66
Table F 1 Data Elements	71
Table F 2 Environmental Risk Factors	79
Table F 3 Example Security Requirements.....	79

FIGURES

Figure 1 Digital Signature	17
Figure 2 Authentication Model	20
Figure 3 Authentication Flow	20
Figure C 1 Synchronous Data Flow.....	59
Figure C 2 Time Synchronous Authentication.....	60
Figure C 3 Time Synchronous Key Management	61
Figure E 1 Access Connection.....	67
Figure F 1 Connectivity.....	70
Figure F 2 Message Flow	70
Figure F 3 Bill Payment Transaction - Payee Setup	72
Figure F 4 Bill Payment Transaction - Payee Delete.....	73
Figure F 5 Bill Payment Transaction - Payment.....	73
Figure F 6 Intra-Bank Transfer Transaction	74
Figure F 7 Balance Inquiry Transaction.....	74
Figure F 8 Loan Application Transaction	75
Figure G 1 Registration Steps.....	81

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, X9 Vice 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

Ferris & Associates

Jean Lovati

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

Merrill Lynch
Moore Business Forms, Inc.
National Association of Convenience Stores
National Security Agency
NCR
New York Clearing House
NOVUS Services, Inc.

Pitney Bowes, Inc.
PricewaterhouseCoopers
SPYRUS

Unisys Corporation

VeriFone, Inc.

VISA International
Wells Fargo Bank
Xcert International, Inc.

Genien Carlson
John Dolan
Thomas Oswald
Robert Swanson
Jerry Rainville
Steve Stevens
Vincent DeSantis
Thomas Kossler
Peggy Douds
David Pratscher
Leon Pintsov
Jeff Zimmerman
Peter Yee
Karen Randall
Tom Hayosh
James Graziano
John Sheets
Brad McGuinness
Trong Nguyen
Stuart Taylor
Bill Chen
Tim Silva
Marc Branchaud
Sandra Lambert

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

Glenda Barnes, Chair
Sandra Lambert, Vice Chair

Cybersafe Corp.
Xcert International, Inc.

Organization Represented

American Bankers Association
American Express Company

Applied Communications Inc.

Bank of America

Bank One Corp.
Bankers Roundtable

Certco LLC

Certicom Corporation
Chase Manhattan Bank

Representative

Kawika Daguio
Bonnie Howard
Glen Weiner
Cindy Rink
Douglas Grote
Mack Hicks
Kathleen Gibbons
Richard Phillips
Martin Johnson
Duane Baldwin
Keviar Warner
Frederick Honold
Richard Ankey
Daniel Geer
Donald Johnson
Gene Rao

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

Northern Telecom, Incorporated
Northstar Technology Group, Inc.
Pitney Bowes, Inc.
PricewaterhouseCoopers

Pulse EFT Association

Racal Guardata, Inc.

SAIC
Security Dynamics
SPYRUS

Technical Communications Corporation
TECSEC Incorporated

US Department of Treasury
VeriFone, Inc

VISA International
Wells Fargo Bank

Xcert International, Inc.

Warwick Ford
John Bowman
Andrei Obrea
John D. Hunt
David Oshman
Jeffrey Zimmerman
Karen Gardstein
Leslie Handrix
Scott Petersen
Emile Soueid
Samuel Epstein
Wanda Gamble-Braggs
Burt Kaliski
Karen Randall
Peter Yee
John Gill
Edward Scheidt
Jay Wack
Gary Grippio
John Sheets
Stuart Taylor
Trong Nguyen
William Chen
Azita Amini
Terry Leahy
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
Azita Amini
Todd Arnold
Glenda Barnes
David Black
Mauro DeFelice
Jim Dray
Jamie Edelkind
Lore Eisenstaedt
Roger Fischer
Jim Foti
Kathleen Gibbons
Sally Graham
Tom Jones
Rick Kastner

Abraham & Associates
Wells Fargo Bank
IBM
Sagus
Sage Technology
Mellon Bank
NIST
Sage Technology, Inc.
Advantis
Norwest Technical Serv.
NIST
Bank of America
Bank of America
Intel
Ernst & Young

Kamy Kavianian
Shirley Kawamoto
George Lundrigan
Debra O'Dell
Rup Parmar
Bill Poletti
Lisa Pretty
John Pratt
Karen Randall
Pud Reaver
Jeff Stapleton
Linda Taylor
Henry Tsui
Jennifer Vancini
Michael Versace

CYLINK
MITRE Corp.
Wayne/Dresser
Lockheed Martin
VanCity Savings CU
MasterCard International
Certicom
EXXON
Spyrus
National Security Agency (NSA)
Security Dynamics
Bank of America
First Data Corp.
Certicom
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