

X9 TG-24-1999

Technical Guideline:
Managing Risk and Migration Planning: Withdrawal of ANSI
X9.9, *Financial Institution Message Authentication Codes (MAC)*
Wholesale

Secretariat

ASC X9, Inc.

Approved: July, 1999

by X9 Committee

Table of Contents

1	SCOPE	1
2	REFERENCES.....	1
3	DEFINITION(S).....	2
4	SYMBOLS (AND ABBREVIATIONS).....	4
5	ORGANIZATION	4
6	RECENT ATTACKS AND THE DATA ENCRYPTION STANDARD (DES).....	5
6.1	THE DATA ENCRYPTION STANDARD (DES).....	5
6.2	THE SUCCESSFUL ATTACK ON DES.....	5
6.3	THE WITHDRAWAL OF ANSI X9.9-1994.....	6
7	REPLACEMENTS FOR THE MAC.....	6
8	UPGRADING WHOLESALE FINANCIAL SYSTEMS TO THE NEW TECHNOLOGY	7
8.1	REPLACING THE X9.9 MACs.....	7
8.2	MANAGING DES AND TRIPLE DES KEYS	8
9	MANAGING RISK DURING THE TRANSITION.....	9
9.1	MANAGING MAC KEYS.....	9
9.2	COMPENSATING CONTROLS IN HIGH RISK SYSTEMS	10
ANNEX A (INFORMATIVE) ATTACKS ON MESSAGES AUTHENTICATED USING THE X9.9 MAC COMPUTATION.....		11
A.1	CIPHERTEXT SOURCE	12
A.2	KNOWN PLAINTEXT SOURCE.....	12
A.3	THE ATTACK.....	12
ANNEX B (INFORMATIVE) CONSIDERATIONS IN ATTACKING X9.17 CRYPTOGRAPHIC SERVICE MESSAGES.....		13
1	WHEN ONE KD IS SENT IN THE RTR (AND, HENCE RSM AND KSM).....	13
1.1	<i>Information available from RTR Messages from the KDC to Party A</i>	<i>13</i>
1.1.1	RTR Contents.....	13
1.1.2	Data input to the Authentication Computation.....	13
1.1.3	Known Result.....	13
1.2	<i>Information available from KSM Messages from Party A to Party B</i>	<i>13</i>
1.2.1	KSM Contents.....	13
1.2.2	Data input to the Authentication Computation.....	13
1.2.3	Known Result.....	13
1.3	<i>The Attack on the MAC</i>	<i>14</i>
2	WHEN TWO KDS ARE SENT IN THE RTR (AND, HENCE RSM AND KSM).....	14
ANNEX C (INFORMATIVE) BIBLIOGRAPHY.....		15

Figures

Figure 1 The X9.9 MAC algorithm 11

Tables

Table 1 Technology available for MAC replacement..... 7

Table 2 Key Agreement and Key Transport 9

Foreword

This Technical Guideline provides information and guidance to users of ANSI X9.9-1994, Financial Institution Message Authentication (Wholesale) on:

- the potential for a successful attack on the DES algorithm when used to compute a Message Authentication Code (MAC) according to ANSI X9.9,
- X9 approved cryptographic tools designed to replace the functionality of X9.9, and
- compensating controls that may reduce the risk of using X9.9 for integrity protection in wholesale systems during the transition to the new cryptographic methods.

Suggestions for improvements to this guideline are welcome. They should be sent to the X9 Secretariat, American Bankers Association, Standards Department, 1120 Connecticut Avenue, N. W., Washington, D. C. 20036. This guideline was processed and approved by the Accredited Standards Committee X9 on Financial Services. Committee approval of this guideline does not imply that all members voted for its approval.

The X9 committee had the following members:

Harold Deal, X9 Chairman
 William Lyons, X9 Vice Chairman
 Cynthia Fuller, Managing Director
 Darlene Schubert, Program Manager

Organization Represented

ACI Worldwide

American Bankers Association
 American Express Company
 Automated Financial Services
 Bank Boston

Banc One Services Corporation
 Bank of America

Canadian Bankers Association

Representative

Douglas Grote
 Cindy Rink
 Anne Livingston
 Bonnie Howard
 Tom Clute
 Frank Jaffe
 Richard Matthews
 Kevin Roden
 William Lyons
 Harold Deal
 Gretchen Breiling
 Christine Arjoonlal
 Mara Bakic

Certicom
Citibank
Cybersafe Corporation
Deloitte & Touche Security Services
Deluxe Corporation
Diebold

Discover Financial Services
Ernst & Young, LLP

Federal Reserve Bank

Ferris & Associates, Inc.
First Data Corporation
Food Marketing Institute
Griffin Consulting
HP/Verifone
IBM Corporation

Intel Corporation
KPMG Peat Marwick LLP

M. Blake Greenlee & Associates, Ltd.
MARS Electronic International

MasterCard International
Mellon Bank, N.A.

Merrill Lynch

National Association of Convenience Stores
National Security Agency
NCR
New York Clearing House
Pitney Bowes, Inc.
PricewaterhouseCoopers
SPYRUS

The Chase Manhattan Bank
Unisys Corporation

Visa International
Wells Fargo Bank
Xcert International

Don Johnson
Seymour Rosen
Glenda Barnes
Jon Graff
Maury Jansen
Sandy Morgan
Mark Covert
Thomas Kossler
Geoffery Turner
Richard Kastner
Ralph Poore
Dexter Holt
Susan Belisle
Martin Ferris
Gene Kathol
Ted Mason
Phillip Griffin
John Sheets
Harry Hankla
Donald Harman
Steve Ellis
Al Van Ranst, Jr.
Jeff Stapleton
Blake Greenlee
E. E. Barnes
Ron Bernardini
Melinda Yee
David Taddeo
Genien Carlson
Ted Gerbracht
John Dolan
Robert Swanson
Gregory Bergren
Steve Stevens
Vincent DeSantis
Leon Pintsov
Jeff Zimmerman
Peter Yee
Karen Randall
Francis Keenan
Thomas Hayosh
James Graziano
Bill Chen
Terry Leahy
Young Etheridge
Marc Branchaud

Sandra Lambert

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

Glenda Barnes, Chairman

Sandra Lambert, Vice Chairman

Organization

ACI Worldwide

Affiliated Computer Services
American Bankers Association
American Express Company

Baltimore Technologies
Bank of America

Bank One Corporation
Certco LLC

Certicom Corporation
Chase Manhattan Bank

Communication Security Establishment

Compaq Computer Corporation
Cybersafe Corporation

Cylink Corporation
DataCard Corporation
Deloitte & Touche Security Services
Deluxe Corporation

Diebold, Inc.

Diversinet Corporation
Entrust Technologies
Ernst & Young, LLP

Representative

Cindy Rink
Dennis Abraham
Douglas J. Grote
Brian Hadaway
Anne Livingston
Bonnie Howard
Glenn Weiner
Lisa Pretty
Mack Hicks
Kathleen Gibbons
Richard Phillips
Martin D. Johnson
Mark Ryding
Daniel Geer
Richard Ankey
Donald Johnson
Gene Rao
Richard Yen
Alan Poplove
Michael Chawrun
Roger French
David O'Brien
Glenda Barnes
Kamy Kavarianian
William Kraetz
Jon Graff
Cory A. Surges
Maury Jansen
Chuck Bram
Sandy Morgan
Mark Covert
Michael Crerar
Robert Zuccherato
Richard Kastner
Ralph Spencer Poore

Federal Reserve Bank

Financial Services Roundtable
First Data Corporation
First Union Corporation

Food Marketing Institute
Fortress Technologies
Gilbarco, Inc.
Griffin Consulting

GTE Internetworking
HP/Verifone
IBM Corporation

IIT Research Institute
Intel Corporation
Jones Futurex
KPMG Peat Marwick LLP
M. Blake Greenlee Associates, Ltd.
Mag-Tek
MasterCard International

Mellon Bank, N.A.
Merrill Lynch

Mitsubishi Electronics America
Motorola
National Association of Convenience Stores
National Security Agency
NCR
NIST

Pitney Bowes, Inc.
PNC Bank
PricewaterhouseCoopers

Pulse EFT Association

Racal Guardata, Inc.

SAIC
Security Dynamics

Richard Sweeney
Michael Versace
Gary Chaulklin
Kit Needham
Gene Kathol
James Ramsey
Sandra Lambert
Ted Mason
Eva Bozoki
Rena Smith
Phillip H. Griffin
Harriette Griffin
Patrick Cain
John Sheets
Harry Hankla
Stephen Mike Matyas
Mohammad Peyravian
Roger Westman
Steve Ellis
Michael Berkowitz
Jeffrey Stapleton
Blake Greenlee
Terry Benson
Ron Karlin
William Poletti
David Taddeo
Lawrence LaBella
Ted Gerbracht
Walter Boyles
Bob Frith
Robert Swanson
Gregory Bergren
Adrian Shields
Donna Dodson
Miles Smid
Andrei Obrea
Tim Garland
John D. Hunt
David Oshman
Jeffrey Zimmerman
Karen Gardstein
Leslie Handrix
Scott Petersen
Samuel Epstein
Wanda Gamble-Braggs
Burt Kaliski

SENSAR
SPYRUS

Technical Communications Corporation
TECSEC Incorporated

US Department of Treasury
VISA International
Wells Fargo Bank

Xcert International, Inc.

Marcos Salganicoff
Karen Randall
Peter Yee
John Gill
Edward M. Scheidt
Jay Wack
Gary Grippo
William Chen
Azita Amini
Terry Leahy
Sandra Lambert
Young Etheridge

Under ASC X9 procedures, X9F oversees the drafting of proposed standards. An ad hoc committee was established by X9F to develop this technical guideline. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The ad hoc committee which developed this technical guideline had the following members:

Gary Chaulklin, Chairman

Organization Represented

M. Blake Greenlee Associates, Ltd
Federal Reserve
Federal Reserve

Representative

Blake Greenlee
Richard Sweeney
Gary Chaulklin

Managing Risk and Migration Planning: Withdrawal of ANSI X9.9 Message Authentication (MAC)

1 Scope

Based on certain attacks on 56 bit DES described in detail in Section 6, it is the consensus of X9 that Message Authentication Codes (MACs) as defined in ANSI X9.9-1994 no longer provide sufficient security to protect wholesale financial transactions. Hence, X9.9 is being withdrawn.

This Guideline discusses:

- using new technology to provide integrity protection for wholesale financial messages,
- transitioning from X9.9 to the new technology, and
- measures can be taken to ameliorate the risk inherent in X9.9 during the transition period.

Please do not misunderstand the intent of this guideline. Continue to use single DES based X9.9 until a replacement is implemented. Until the replacement is implemented, there are actions that can be taken to reduce the risks associated with implementations of X9.9.

2 References

- [1] ANSI X9.9-1994, *Financial Institution Message Authentication (Wholesale)*.
- [2] ANSI X9.17-1995, *Financial Institution Key Management (Wholesale) (being withdrawn)*
- [3] ANSI X9.71-199x, *Keyed Hash for Message Authentication (nearing ballot)*.
- [4] ANSI X9.72-199x, *Peer Entity Authentication Using Public Key (nearing ballot)*.
- [5] ANSI X9.30-1997, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)*.
- [6] ANSI X9.30-1993, Part 2: *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: The Secure Hash Algorithm 1 (SHA-1) (Revised)*.

- [7] ANSI X9.31-1998, *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, The rDSA Algorithm.*
- [8] ANSI X9.42 – 199x, *Public Key Cryptography for The Financial Service Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithm (nearing ballot)*
- [9] ANSI X9.44-199x, *The Transport of Symmetric Algorithms Keys Using Reversible Public Key Cryptography (in preparation)*
- [10] ANSI X9.52-1998, *Triple Data Encryption Algorithms Modes of Operation*
- [11] ANSI X9.62-1998, *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).*
- [12] ANSI X9.63-199x, *Key Agreement and Key Transport Using Elliptic Curve-Based Cryptography (nearing ballot)*
- [13] ISO DIS 15782, *Banking – Certificate Management Part 1: Public Key Certificates*
- [14] ISO DIS 15782, *Banking – Certificate Management Part 3: Certificate Extensions*

3 Definition(s)

1. Advanced Encryption Standard (AES)

The future Advanced Encryption Standard (AES) which is in development as a DES replacement by NIST (National Institute of Standards and Technology).

2. Asymmetric Cryptographic Algorithm

A cryptographic algorithm that uses two related keys, a public key and a private key; the two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

3. Certification Authority (CA)

A Center trusted by one or more entities to create and assign certificates

4. Cryptographic Hash Function

A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. The function satisfies the following properties:

- a. it is computationally infeasible to find any input which maps to any pre-specified output;
- b. it is computationally infeasible to find any two distinct inputs which map to the same output.

4. Cryptographic Key

A parameter that determines the operation of a cryptographic function such as:

- a. the transformation from plaintext to ciphertext and vice versa,
- b. the synchronized generation of keying material,
- c. a digital signature computation or verification.

5. Cryptography

The discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use, or a combination thereof.

6. Cryptoperiod

The time span during which a specific key is authorized for use or in which the keys for a given system may remain in effect.

7. Digital Signature

A cryptographic transformation of data which, when associated with a data unit, provides the services of:

- origin authentication;
- data integrity; and

may support signer non-repudiation.

8. Elliptic Curve Digital Signature Algorithm

.Refer to ANSI X9.62, Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

9. Financial Message

A communication containing information which has financial implications.

10. Message

The data to be signed.

11. Message Authentication

The verification of the source, uniqueness and integrity of a message as specified in ANSI X9.9-1986.

12. Message Authentication Code (MAC)

A cryptographic value which is the results of passing a financial message through the message authentication algorithm using a specific key.

13. Private key

In an asymmetric (public) key system, that key of an entity's key pair which is known only by that entity.

14. Public key

In an asymmetric key system, that key of an entity's key pair which is publicly known.

15. Public Key Certificate

The public key and identity of an entity together with some other information rendered unforgeable by signing the certificate information with the private key of the certifying authority that issued that public key certificate.

16. Secure Hash Algorithm, Revision 1 (SHA-1)

SHA-1 implements a hash function which maps messages of a length less than 2^{64} bits to hash values of a length which is exactly 160 bits.

16. Triple DES

The methods for obtaining increased security by repetitive use of the DES algorithm as defined in ANSI X9.52-1998, *Triple Data Encryption Algorithms Modes of Operation*.

4 Symbols (and abbreviations)

Abbreviation	Meaning
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
MAC	Message Authentication Code
MID	Message Identifier.
rDSA	Reversible Digital Signature Algorithm
SHA-1	Secure Hash Algorithm-1

5 Organization

The following Informative annexes give additional information which may be useful to users of this Guideline.

Annex	Contents
A	Attacks on Authenticated Messages Using the X9.9 MAC Computation
B	Considerations in Attacking X9.17 Cryptographic Service Messages
C	Bibliography

6 Recent Attacks and The Data Encryption Standard (DES)

6.1 The Data Encryption Standard (DES)

The Data Encryption Standard DES was designed by IBM and was accepted as a Federal Information Processing Standard (FIPS 46) by NIST in 1977. As a government algorithm, it is used for the protection of sensitive unclassified data. In 1981, DES was adopted as an American National Standard, X3.92. It was quickly adopted as the algorithm preferred by the financial community, worldwide.

DES has protected financial and unclassified government communications for twenty years. At the present time, it is the most widely used algorithm, worldwide. DES uses a 56-bit key to encrypt a 64-bit block.

All encryption algorithms, including DES, have a key exhaustion strength, which is the expected amount of computation needed to try every possible key to determine which one is the correct key. Increases in computational capabilities and in mathematical analysis of an encryption algorithm should be expected to necessitate increasing the key size to resist key exhaustion (and similar) attacks. The key exhaustion strength of DES is over 72 quadrillion possible keys.

6.2 The Successful Attack on DES

On July 17, 1998, the New York Times reported that a group of computer experts had succeeded in breaking the Data Encryption Standard (DES) by building a cracking machine costing \$250,000. The machine, consisting of 27 boards each holding 64 chips comprising a total of 37050 search units, takes an average of 112 hours to search through half the key space and decipher an encrypted message. The machine performs a key exhaustion attack in which possible keys are tested one at a time until the correct key is found. This was not the first time that a DES key had been recovered by a key exhaustion attack. However, previous attacks took several months and involved the use of thousands of computers administered by many different organizations.

In fact, a book, *Cracking DES: Secrets of Encryption Research, Wiretap Politics, & Chip Design*, has been published by O'Reilly and Associates. Details may also be found on the Electronic Frontier Foundation (EFF) web site, <http://www.eff.org>. The book provides all technical specifications needed to build a DES Cracker.

The type of attack used to attack DES is called a known plaintext attack, where it is assumed the attacker knows a few (say, 2 or 3) 64-bit blocks of plaintext/ciphertext pairs. In practice, this is often the case as messages have structure or a particular encoding scheme (i.e. ASCII). It is always the case when a MAC is used to provide integrity protection to a plaintext message. Thus, it is a conservative assumption to make that an adversary will be able to determine some known plaintext encrypted by a specific DES key and thus the requirements needed to execute the attack will be met.

This most recent attack demonstrates that a single determined attacker can build an effective DES cracking machine.

6.3 The withdrawal of ANSI X9.9-1994

This attack can be used to derive the cryptographic key used to compute MACs.

Because of the ability of an adversary to successfully derive a single DES key using a known plaintext attack, ANSI X9.9 is being withdrawn.

Annex “A” shows the concepts of using this method of attacking a MAC to derive the key.

7 Replacements for the MAC

Several years ago, when it was determined that the DES was approaching the end of its useful life, Accredited Standards Committee X9 (whose members include NIST and the National Security Agency), began work on a family of standards that would provide financial message security. Refer to the References section for the status of these standards. These standards:

1. ANSI X9.71-199x, *Keyed Hash for Message Authentication*.
2. ANSI X9.72-199x, *Peer Entity Authentication Using Public Key*.
3. ANSI X9.30-1997, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)*.
4. ANSI X9.30-1993, Part 2: *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: The Secure Hash Algorithm 1 (SHA-1) (Revised)*.
5. ANSI X9.31-1998, *Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, The rDSA Algorithm*.
6. ANSI X9.42 – 199x, *Public Key Cryptography for The Financial Service Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithm*
7. ANSI X9.44-199x, *The Transport of Symmetric Algorithms Keys Using Reversible Public Key Cryptography*
8. ANSI X9.52-1998, *Triple Data Encryption Algorithms Modes of Operation*
9. ANSI X9.62-1998, *Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*.

10. ANSI X9.63-199x, *Key Agreement and Key Transport Using Elliptic Curve-Based Cryptography*

are based on public key cryptography and the use of hash algorithms.

The use of public key certificates and digital signature algorithms is defined in:

1. ISO DIS 15782, *Banking – Certificate Management Part 1: Public Key Certificates*, and
2. ISO DIS 15782, *Banking – Certificate Management Part 3: Certificate Extensions*.

8 Upgrading wholesale financial systems to the new technology

8.1 Replacing the X9.9 MACs

Table 1, below, provides information on the technology available for MAC replacement. Refer to the Reference section for the status of these standards.

Table 1 Technology available for MAC replacement

Standard	Protection provided	Comments
ANSI X9.19-1998, <i>Financial Institution Retail Message Authentication</i>	Integrity	An option to use a two key, three encryption DEA scheme to prevent exhaustive key determination.
ANSI X9.71-199x, <i>Keyed Hash for Message Authentication</i>	Integrity	Easily implemented; uses ANSI X9.30-1993, Part 2: Public key cryptography using irreversible algorithms for the financial services industry: The Secure Hash Algorithm 1 (SHA-1) (Revised) to compute the hash. Sending and receiving parties must share the same key.
ANSI X9.30-1997, <i>Public Key Cryptography Using Irreversible Algorithms for</i>	Integrity	Recipients of signed messages must have a copy of the sending party's

Standard	Protection provided	Comments
<i>the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA).</i>		public key.
ANSI X9.31-1998, <i>Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, The rDSA Algorithm</i>	Integrity	Recipients of signed messages must have a copy of the sending party's public key.
ANSI X9.62-1998, <i>Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)</i>	Integrity	Recipients of signed messages must have a copy of the sending party's public key.
ISO DIS 15782, <i>Banking – Certificate Management Part 1: Public Key Certificates</i>	Supports: 1. integrity and provides the cryptographic tools to support non-repudiation and 2. authenticating keys used for key agreement and key transport.	Provides the mechanism for distributing authenticated copies of public keys.
ISO DIS 15782, <i>Banking – Certificate Management Part 3: Certificate Extensions</i>		Defines how extensions to public key certificates are to be used.

8.2 Managing DES and Triple DES keys

DES and Triple DES keys must be managed. While ANSI X9.17, Financial Institution Key Management (Wholesale) is specifically designed so that users can change single DES keys easily, it was never designed to protect keys against a known plaintext attack. The frequency of key changes should be related to the business risk.

Implementations of Triple DES, as defined in ANSI X9.52 and the future Advanced Encryption Standard (AES) which is in development as a Triple DES replacement by

NIST should upgrade to key management as defined in Table 2. Refer to the Reference section for the status of these standards.

Table 2 Key Agreement and Key Transport

Standard	Comments
ANSI X9.42 – 199x, <i>Public Key Cryptography for The Financial Service Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithm</i>	Provides a variety of schemes based on Diffie Hellman and the new MQV algorithm.
ANSI X9.63-199x, <i>Key Agreement and Key Transport Using Elliptic Curve-Based Cryptography</i>	Provides: 1. a variety of schemes based on Diffie Hellman and the new MQV algorithm. Provides equivalent security to that defined in X9.42 and X9.44 with substantial reduction in key lengths. Optionally, can be used for key agreement or key transport.
ANSI X9.44-199x, <i>The Transport of Symmetric Algorithms Keys Using Reversible Public Key Cryptography</i>	Uses the RSA or Rabin-Williams algorithms for key transport.

9 Managing risk during the transition

For some systems and types of data, the risk to valuable data is high, and immediate remedial steps are necessary. In other cases the attack may not pose an immediate or significant threat. Therefore, a prudent transition period may be necessary.

9.1 Managing MAC keys

ANSI X9.17-1995, *Financial Institution Key Management (Wholesale)* which is used to manage the data keys for MAC computation was not designed to protect data keys against a known plaintext attack (the data keys are used to compute the MAC on the Cryptographic Service Message). Hence, frequent key changes, with a goal of one key per financial message is the only compensating control available..

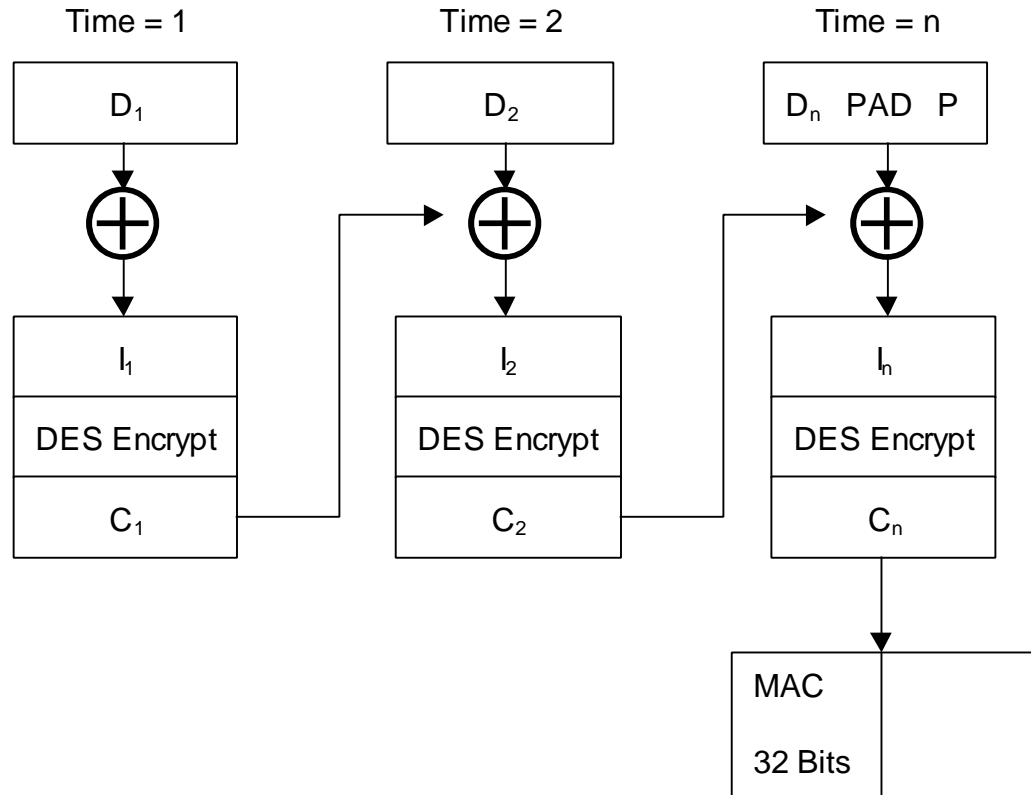
The *KK option in X9.17 should be used.

9.2 Compensating controls in high risk systems

1. Initiate key changes as frequently as is operationally feasible. The goal should be a new key for each session or transaction.
2. Utilize normal, prudent controls that look for duplicate transactions, and payments or payment requests that exceed norms or initiate from unusual sources.
3. Maintain accurate and detailed audit journals – which can be used in investigations of potential fraud attempts and in the recovery of losses.

Annex A (Informative) Attacks on Messages Authenticated Using the X9.9 MAC Computation

Figure 1, below, shows the X9.9 MAC algorithm.



Legend:	
D_t	= Data block at time t
I_t	= Intermediate value block at time t
C_t	= Cipher Block at time t
IV	= 64 bit Initialization Vector
PAD	= (P-1) Padding Characters
P	= Padding Count
\oplus	= Exclusive-OR

Figure 1 The X9.9 MAC algorithm

A.1 Ciphertext Source

The ciphertext is the MAC

A.2 Known Plaintext Source

The plaintext is the message.

A.3 The Attack

According to the HAC¹, “an exhaustive attack reduces the key space to about 2^{24} possibilities. However, ..., a second text-MAC pair almost certainly determines a unique MAC key.”

The number of encryption operations per trial is approximately:

[the number of bytes in the financial message]/8

A second message authenticated using the same key supplies sufficient information to mount the attack with a high degree of certainty.

¹ Handbook of Applied Cryptography, P-354.

