

X9 TG-25-1999

Technical Guideline:
Managing Risk and Migration Planning: Withdrawal of ANSI
X9.23, *Encryption of Wholesale Financial Messages*

Secretariat

ASC X9, Inc.

Approved 1999

by X9 Committee

Table of Contents

1	SCOPE	1
2	REFERENCES.....	1
3	DEFINITION(S).....	3
4	SYMBOLS (AND ABBREVIATIONS).....	4
5	ORGANIZATION	5
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 X9.23-1995.....	6
7	REPLACEMENTS FOR X9.23	6
8	UPGRADING WHOLESALE FINANCIAL SYSTEMS TO THE NEW TECHNOLOGY	7
8.1	REPLACING THE X9.23 ENCRYPTION	7
8.2	MANAGING DES AND TRIPLE DES KEYS	7
9	MANAGING RISK DURING THE TRANSITION.....	9
9.1	THE CONCEPT OF SECURITY LIFE	9
9.2	MANAGING ENCRYPTION KEYS.....	10
9.3	COMPENSATING CONTROLS IN HIGH RISK SYSTEMS	10
	ANNEX A (INFORMATIVE) ATTACKS ON MESSAGES ENCRYPTED USING X9.23	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
B.1	WHEN ONE KD IS SENT IN THE RTR (AND, HENCE RSM AND KSM).....	13
B.1.1	<i>Information available from RTR Messages from the KDC to Party A.....</i>	<i>13</i>
B.1.1.1	RTR Contents.....	13
B.1.1.2	Data input to the Authentication Computation.....	13
B.1.1.3	Known Result.....	13
B.1.2	<i>Information available from KSM Messages from Party A to Party B.....</i>	<i>13</i>
B.1.2.1	KSM Contents.....	13
B.1.2.2	Data input to the Authentication Computation.....	13
B.1.2.3	Known Result.....	13
B.1.3	<i>The Attack on the MAC.....</i>	<i>14</i>
B.2	WHEN TWO KDS ARE SENT IN THE RTR (AND, HENCE RSM AND KSM).....	14
	ANNEX C (INFORMATIVE) BIBLIOGRAPHY.....	15

1	SCOPE	1
2	REFERENCES.....	1
3	DEFINITION(S).....	3
4	SYMBOLS (AND ABBREVIATIONS)	4
5	ORGANIZATION	5
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 X9.23-1995.....	6
7	REPLACEMENTS FOR X9.23	6
8	UPGRADING WHOLESALE FINANCIAL SYSTEMS TO THE NEW TECHNOLOGY	7
8.1	REPLACING THE X9.23 ENCRYPTION	7
8.2	MANAGING DES AND TRIPLE DES KEYS	7
9	MANAGING RISK DURING THE TRANSITION.....	9
9.1	THE CONCEPT OF SECURITY LIFE	9
9.2	MANAGING ENCRYPTION KEYS.....	10
9.3	COMPENSATING CONTROLS IN HIGH RISK SYSTEMS	10
	ANNEX A (INFORMATIVE) ATTACKS ON MESSAGES ENCRYPTED USING X9.23	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 X9.23 Cipher Block Chaining Algorithm..... 11

Tables

Table 1 Technology available for encryption..... 7

Table 2 Key Agreement and Key Transport Algorithms 8

Table 3 Authenticating key agreement and key transport..... 8

Table 4 Protocols for key management and confidentiality protection 9

Foreword

This Technical Guideline provides information and guidance to users of ANSI X9.23-1995, *Encryption of Wholesale Financial Messages* on:

- the potential for a successful attack on the DES algorithm given either a plaintext cipher text pair or a known message structure (i.e. ASCII),
- X9 approved cryptographic tools designed to replace the functionality of X9.23, and
- compensating controls that may reduce the risk of using X9.23 for confidentiality 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

A special thanks to the following individuals who also contributed to this Technical Guideline:

Organization Represented

NCR
TECSEC

Representative

Adrian Shields
Ed Scheidt
Pud Reaver

Managing Risk and Migration Planning: ANSI X9.23 Encryption of Wholesale Financial Messages

1 Scope

Based on certain attacks on 56 bit DES described in detail in chapter 6, it is the consensus of X9 that ANSI X9.23-1995 no longer provides sufficient security to protect wholesale financial transactions. Hence, X9.23 is being withdrawn.

This Guideline discusses:

- using new technology to provide integrity protection for wholesale financial messages,
- transitioning from X9.23 to the new technology, and
- measures can be taken to ameliorate the risk inherent in X9.23 during the transition period.

Please do not misunderstand the intent of this guideline. Continue to use single DES based X9.23 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 X9.23.

2 References

- [1] ANSI X9.23-1995, *Encryption of Wholesale Financial Messages*.
- [2] ANSI X9.17-1995, *Financial Institution Key Management (Wholesale)*
- [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 (nearing ballot)*
- [7] ANSI X9.44-199x, *The Transport of Symmetric Algorithms Keys Using Reversible Public Key Cryptography (in preparation)*
- [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 (nearing ballot)*
- [11] ANSI X9.70-199x, *Symmetric Key Distribution Using Public Key (nearing ballot)*
- [12] ANSI X9.71-199x, *Keyed Hash for Message Authentication (nearing ballot).*
- [13] ANSI X9.72-199x, *Peer Entity Authentication Using Public Key (nearing ballot).*
- [14] ANSI X9.73-199x, *Cryptographic Message Syntax (nearing ballot)*
- [15] ANSI X9.77-199x, *Public Key Infrastructure Protocols (in preparation)*
- [16] ISO DIS 15782, *Banking – Certificate Management Part 1: Public Key Certificates*
- [17] ISO DIS 15782, *Banking – Certificate Management Part 3: Certificate Extensions*
- [18] ANSI TG-19-1, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures*
- [19] ANSI X9.65-199x, *Triple Data Encryption Algorithm (TDEA) Implementation (nearing ballot)*
- [20] ANSI X9.69-1999, *Framework for Key Management Extensions (being published)*
- [21] ANSI X3.92-1981 *Data Encryption Algorithm*
- [22] *FIPS 46-2 Data Encryption Standard*

3 Definition(s)

1. 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.

2. Certification Authority (CA)

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

3. 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:

1. it is computationally infeasible to find any input which maps to any pre-specified output;
2. 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:

1. the transformation from plaintext to ciphertext and vice versa,
2. the synchronized generation of keying material,
3. 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. Encryption

A process of transforming plain text (readable) into cipher text (unreadable) for the purpose of security or privacy.

10. Financial Message

A communication containing information which has financial implications.

11. Message

The data to be signed.

12. Private Key

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

13. Public Key

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

14. 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.

15. 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. Security Life

The time span over which cryptographically protected data have value.

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 Encrypted Data Using the X9.23
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 accepted as a Federal Information Processing Standard (FIPS 46-2) by the National Institute of Standards and Technology (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 that are known to an attacker, 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. Armed with only the knowledge of the plaintext's encoding scheme (i.e. ASCII), the attacker is able to mount a successful attack. Thus, it is a conservative assumption to make that an adversary will be able to determine some known plaintext or encoding scheme 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 X9.23-1995

A brute force attack can now be used to derive the cryptographic key used to encrypt messages using the method of ANSI X9.23.

Because of the ability of an adversary to successfully derive a single DES key using a known plaintext attack and the subsequent loss of message confidentiality, ANSI X9.23 is being withdrawn.

Annex A shows the concepts of using this method of attacking a message to derive the key.

7 Replacements for X9.23

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 the National Institute for Standards and Technology (NIST) and the National Security Agency (NSA)), began work on a family of standards that would provide financial message security. These standards ([8], [18], and [19]) are based on three iterations of the Data Encryption Algorithm (DEA), known as triple DEA.

8 Upgrading wholesale financial systems to the new technology

8.1 Replacing the X9.23 encryption

Table 1, below, provides information on the technology available for replacement of DES as an encryption algorithm. Refer to the References section for the status of these standards and guidelines.

Table 1 Technology available for encryption

Standard	Comments
ANSI X9.52-1998, <i>Triple Data Encryption Algorithms Modes of Operation</i>	Interim replacement for DES until the Advanced Encryption Standard (AES) is available - see below. Provides 112 bits of security
ANSI TG-19-1, <i>Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures</i>	Implementations of X9.52 may be validated using TG-19-1
ANSI X9.65, Triple Data Encryption Algorithm (TDEA) Implementation	Provides secure implementation strategies for X9.52

The Advanced Encryption Standard (AES) is under development at NIST To provide an easy transition to the AES when that algorithm is available, implementations of Triple DES should be algorithm independent. The minimum acceptability requirements of AES can be found at http://csrc.nist.gov/encryption/aes/aes_9709.htm#sec3. The AES home page is http://csrc.nist.gov/encryption/aes/aes_home.htm. The minimum key size is 128 bits and the minimum input/output block size is 128. Other key and block sizes must be supported as well. The algorithm must be a secret key, block cipher. Refer to the information at the NIST site for the exact details and the status of the AES initiative.

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 and future AES implementations should upgrade to the key agreement and key transport algorithms as defined in Table 2. Table 3 lists standards

that define the means to authenticate the delivery of keys. Table 4 lists protocol and messaging standards that should also be used in this upgrade process. Refer to the References section for the status of these standards and guidelines.

Table 2 Key Agreement and Key Transport Algorithms

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: <ol style="list-style-type: none"> 1. a variety of schemes based on Diffie Hellman and the new MQV algorithm. 2. Provides equivalent security to that defined in X9.42 and .X9.44 with substantial reduction in key lengths. 3. 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</i>	Uses the RSA or Rabin-Williams algorithms for key transport.

Table 3 Authenticating key agreement and key transport

Standard	Comments
ANSI X9.30-1997, <i>Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry, Part 1: The Digital Signature Algorithm (DSA)</i> .	Recipients of signed messages must have a copy of the sending party's public key.
ANSI X9.31-1998, <i>Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry, The rDSA Algorithm</i>	Recipients of signed messages must have a copy of the sending party's public key.
ANSI X9.62-1998, <i>Public Key</i>	Recipients of signed messages must have

Standard	Comments
<i>Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)</i>	a copy of the sending party's public key.
ISO DIS 15782, <i>Banking – Certificate Management Part 1: Public Key Certificates</i>	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.

Table 4 Protocols for key management and confidentiality protection

Standard	Comments
ANSI X9.70-199x, <i>Symmetric Key Distribution Using Public Key</i>	
ANSI X9.73-199x, <i>Cryptographic Message Syntax</i>	
ANSI X9.77-199x, <i>Public Key Infrastructure Protocols</i>	
ANSI X9.69-1999, <i>Framework for Key Management Extensions</i>	

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 advisable.

9.1 The concept of security life

Security life is the time span over which cryptographically protected data have value. Transactions in on-line wire transfer systems have security lives that are measured in seconds. Data for mergers and acquisitions, corporate plans and marketing strategies typically have much longer security lives. Some information in multi-national financial institutions has a security life measured in decades.

Since it has been demonstrated that \$250,000 in hardware can derive a DES key in 56 hours, and that number is a linear function of the number of hardware machines purchased, it is no longer prudent to trust high risk financial and management information that has a security life of over a few minutes to a system protected by single DES.

For the most sensitive information, manual means, with appropriate controls should be used.

9.2 Managing encryption 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. Annex B discusses considerations in attacking X9.17 Cryptographic Service Messages.

During the transition to new technology, the Triple DES key management option in X9.17 should be used.

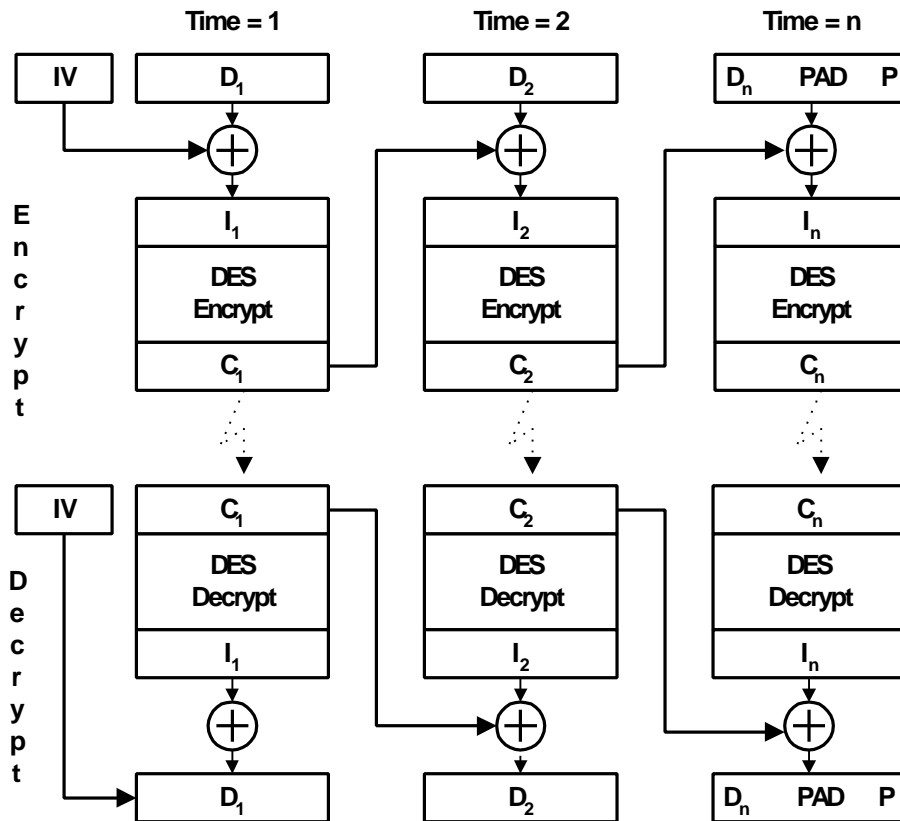
9.3 Compensating controls in high risk systems

Immediately:

1. Initiate key changes as frequently as is operationally feasible. The goal should be a new key for each session or transaction.
2. Cease using DES to protect information that must be kept confidential for any times over a minute.
3. Use the *KK option in X9.17 for key management
4. 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 Encrypted Using X9.23

Figure 1, below, shows the X9.23 encryption.



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
- ⊕ = Exclusive-OR

Figure 1 The X9.23 Cipher Block Chaining Algorithm

A.1 Ciphertext Source

C_2 , the output of the second block cipher operation is the ciphertext.

A.2 Known Plaintext Source

As most bank messages are highly structured, and that structure is known, D_2 is known. Since C_1 is transmitted, it is also known. Then, the known plaintext is:

$$(D_2 + C_1) \text{ modulo } 2.$$

A.3 The Attack

The attack is a straight forward known plaintext attack or knowledge of the message encoding scheme using equipment such as that designed for the DES Challenge.

Annex B
(informative)
**Considerations in Attacking X9.17 Cryptographic
Service Messages**

B.1 When one KD is sent in the RTR (and, hence RSM and KSM)

B.1.1 Information available from RTR Messages from the KDC to Party A

B.1.1.1 RTR Contents

MCL/RTR**b**KSM**b**RCV/RRRR**b**ORG/OOOO**b**IDU/UUUU**b**KD/[ede*KN(KDI)
(optional subfields)]**b**KDU/[ede*KN(KD) (optional
subfields)]**b**IV/[E||eKDH(IV)]**b**CTB/**b**CTA/**a**MAC/[aKDJ(MCL/RTR/ b...
bCTA/x**b**]

Here, the data key used to compute the MAC is the data key sent in the message. With high probability, a candidate pool of approximately 16,777,216 possible KDs can be determined by a known plain text attack against the CSM using the following input to the MAC process:

B.1.1.2 Data input to the Authentication Computation

MCL/RTR**b**KSM**b**RCV/RRRR**b**ORG/OOOO**b**IDU/UUUU**b**KD/[ede*KN(KDI)
(optional subfields)]**b**KDU/[ede*KN(KD) (optional subfields)]**b**IV/[E ||
eKDH(IV)]**b**CTB/**b**CTA/**a**

B.1.1.3 Known Result

MAC/[aKDJ(MCL/RTR/ b... bCTA/x**b**)] = a 32 bit string

B.1.2 Information available from KSM Messages from Party A to Party B

B.1.2.1 KSM Contents

MCL/KSM**b**RCV/RRRR**b**ORG/OOOO**b**IDC/CCCC**b**KDU/[KDUC (optional
subfields)]**b**IV/IVC**b**CTB/**b**MAC/[aKDJ(MCL/KSM**b**... **b**CTB/x**b**)]

B.1.2.2 Data input to the Authentication Computation

MCL/KSM**b**RCV/RRRR**b**ORG/OOOO**b**IDC/CCCC**b**KDU/[KDUC (optional
subfields)]**b**IV/IVC**b**CTB/**b**

B.1.2.3 Known Result

MAC/[aKDJ(MCL/KSM**b**... **b**CTB/x**b**)]

B.1.3 The Attack on the MAC

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:

$$[\text{the number of bits in the KSM (less the MAC field)}/8]$$

Assuming that a single KD is sent in each Cryptographic Service Message, a single RTR/KSM or KSM/RSM pair supplies sufficient information to mount the attack.

B.2 When two KDs are sent in the RTR (and, hence RSM and KSM)

If two KDs are sent from the CKD, say KDA and KDB, the key used to compute the MAC in the RTR, the RSM and the KSM is:

$KDC = (KDA + KDB)$, where + denotes a bitwise Boolean exclusive OR operation.

An attack on MAC computed using this composite will determine KDC, but not the underlying KDA and KDB. However, if one of the keys can be determined by attacking a message authenticated using, say, KDA, then KDB can be determined by simply computing the modulo 2 sum of KDA and KDC.

¹ Handbook of Applied Cryptography, P-354.

Annex C
(informative)
Bibliography

- [1] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.