Contents

Foreword .................................................................................................................................................. v
Introduction ........................................................................................................................................ vi
1 Scope .................................................................................................................................................. 1
2 References ......................................................................................................................................... 1
3 Terms and definitions ....................................................................................................................... 2
4 Symbols and abbreviated terms ........................................................................................................ 3
5 Key Block Properties and Characteristics .......................................................................................... 5
  5.1 Key Block Elements .................................................................................................................... 5
  5.2 Confidential Data to be Exchanged/Stored .................................................................................. 5
  5.3 Key Block Binding and Validation Methods ............................................................................... 5
    5.3.1 General .................................................................................................................................... 5
    5.3.2 Key Block Binding Method Using Key Derivation (Preferred) .............................................. 5
    5.3.3 Key Block Binding Method Using Variants ......................................................................... 9
Annex A CBC MAC Key Block with Optional Block ............................................................................ 11
  A.1 Introduction ............................................................................................................................... 11
  A.2 Key Block Header (KBH) .......................................................................................................... 11
  A.3 Encryption .................................................................................................................................. 14
    A.3.1 Encryption Using Key Derivation Binding Method .............................................................. 14
    A.3.2 Encryption Using Key Variant Binding Method ................................................................. 14
  A.4 MAC ........................................................................................................................................... 15
    A.4.1 MAC Using Key Variant Binding Method ........................................................................... 15
    A.4.2 MAC Using Key Derivation Binding Method .................................................................... 15
  A.5 Defined values for Key Block Headers ..................................................................................... 15
    A.5.1 Key Usage ............................................................................................................................. 15
    A.5.2 Algorithm ............................................................................................................................... 18
    A.5.3 Mode of Use ........................................................................................................................... 18
    A.5.4 Key Version Number ............................................................................................................. 20
    A.5.5 Exportability .......................................................................................................................... 20
    A.5.6 Optional block ID .................................................................................................................. 21
  A.6 Encoding ...................................................................................................................................... 23
  A.7 Key Block Examples ................................................................................................................... 24
    A.7.1 Notation Used .......................................................................................................................... 24
    A.7.2 Example 1: Key Block without Optional Blocks .............................................................. 24
    A.7.3 Example 2: Key Block with Optional Block ..................................................................... 37
  A.8 The CMAC mode for authentication .......................................................................................... 50
    A.8.1 Introduction ............................................................................................................................. 50
    A.8.2 Subkey derivation .................................................................................................................... 51
    A.8.3 MAC generation with CMAC ............................................................................................. 54
    A.8.4 MAC Verification with CMAC ............................................................................................ 57
Annex B Process for Approval of New Field Values ............................................................................ 58
  B.1 Introduction .................................................................................................................................... 58
  B.2 Origination .................................................................................................................................... 58
  B.3 Justification for Proposal ............................................................................................................. 58
  B.4 Examination of Proposals ........................................................................................................... 58

© 2010 I All rights reserved i
B.5 Appeals Procedure.........................................................................................................................59
B.6 Approved List Of Key Block Field Values .....................................................................................59
B.7 TR-31 Revision ...............................................................................................................................59
Annex C New Field Value Request Form.............................................................................................60
Figures

Figure 1  Deriving a 2-Key TDEA MAC and Encryption Key ................................................................. 7
Figure 2  Deriving a 3-Key TDEA MAC and Encryption Key ................................................................. 7
Figure 3  Key Block Binding Method ...................................................................................................... 8
Figure 4  CBC MAC Key Block ............................................................................................................... 11
Figure 5  Examples of KBH and Optional Blocks .................................................................................. 22
Figure 6  CMAC Subkey Derivation from the Key Block Protection Key .................................................. 30
Figure 7  Deriving the Key Block Encryption Key from the Key Block Protection Key ....................... 31
Figure 8  Derivation of the Key Block MAC Key from the Key Block Protection Key ......................... 32
Figure 9  CMAC Subkey Derivation from the Key Block MAC Key ....................................................... 33
Figure 10  Calculation of the MAC over the Header and the Binary Key Data ....................................... 34
Figure 11  Encrypting the confidential data ............................................................................................. 36
Figure 12  CMAC Subkey Derivation from the Key Block Protection Key ................................................ 43
Figure 13  Deriving the Key Block Encryption Key from the Key Block Protection Key ....................... 44
Figure 14  Derivation of the Key Block MAC Key from the Key Block Protection Key ......................... 45
Figure 15  CMAC Subkey Derivation from the Key Block MAC Key ....................................................... 46
Figure 16  Calculation of the MAC over the Header and the Key Data .................................................... 48
Figure 17  Encrypting the confidential data ............................................................................................. 49
Figure 18  CMAC process overview ....................................................................................................... 51
Figure 19  CMAC Subkey Derivation for TDEA ..................................................................................... 52
Figure 20  CMAC Subkey Derivation for AES ......................................................................................... 54
Figure 21  Calculating the MAC with CMAC, Case a ............................................................................. 56
Figure 22  Calculating the MAC with CMAC, Case b ............................................................................. 57

Tables

Table 1  Key Derivation Input Data ........................................................................................................ 5
Table 5-2. Encryption IV ....................................................................................................................... 9
Table A-1. KBH for CBC MAC Binding Method .................................................................................. 12
Table A-2. Example of confidential data for a double-length TDEA key............................................................... 14
Table A-3. Defined Key Usage Values ............................................................................................................... 15
Table A-4. Defined Algorithm Values.................................................................................................................. 18
Table A-5. Defined Mode of Use Values............................................................................................................. 19
Table A-6. Key Version Number definition........................................................................................................ 20
Table A-7. Defined Values for Exportability Byte ................................................................................................ 20
Table A-8. Defined Values for Optional Block ID ................................................................................................ 23
Table A-9. Key Block Values Version IDs Optional Block ................................................................................... 23
Table 10 δ Values for Example............................................................................................................................ 32
Table 11 δ Values for Example............................................................................................................................ 45
Foreword

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Committee X9, Incorporated, 1212 West Street, Suite 200, Annapolis, MD 21401. This document is registered as a Technical Report according to the “Procedures for the Registration of Technical Reports with ANSI.” This document is not an American National Standard and the material contained herein is not normative in nature. Comments on the content of this document should be sent to: Attn: Executive Director, Accredited Standards Committee X9, Inc., 1212 West Street, Suite 200, Annapolis, MD 21401.

CAUTION NOTICE: This Technical Report 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 technical report no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
1212 West Street, Suite 200
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Copyright © 2010 ASC 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. Published in the United States of America.
Introduction

The retail financial transactions industry has in the past lacked an interoperable method for secure key exchange. While this has always been an issue, the move from Single DES to Triple DEA (TDEA) encryption made this issue more acute, as methods for the secure exchange of TDEA keys are non-obvious. This Technical Report is intended to give the reader an implementation that meets the requirements for secure key management as set forth in ANS X9.24 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques.

NOTE The user's attention is called to the possibility that compliance with this technical report may require use of an invention covered by patent rights.

By publication of this technical report, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

Suggestions for the improvement or revision of this Technical Report are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 1212 West Street, Suite, Annapolis, MD 21401 USA.

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

The X9 committee had the following members:
Roy DeCicco, X9 Chairman
Claudia Swendseid, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Janet Busch, Program Manager

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACI Worldwide</td>
<td>Doug Grote</td>
</tr>
<tr>
<td>American Bankers Association</td>
<td>C. Diane Poole</td>
</tr>
<tr>
<td>American Express Company</td>
<td>Ted Peirce</td>
</tr>
<tr>
<td>Apriva</td>
<td>Len Sutton</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Daniel Welch</td>
</tr>
<tr>
<td>Certicom Corporation</td>
<td>Daniel Brown</td>
</tr>
<tr>
<td>Citigroup, Inc.</td>
<td>Karla McKenna</td>
</tr>
<tr>
<td>CUSIP Service Bureau</td>
<td>James Taylor</td>
</tr>
<tr>
<td>Deluxe Corporation</td>
<td>Ralph Stolp</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Bruce Chapa</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Michelle Zhang</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Claudia Swendseid</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Rick Van Luvender</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Skip Smith</td>
</tr>
</tbody>
</table>
At the time it approved this standard, the X9F Subcommittee on Data and Information Security had the following members:

Ed Scheidt Chairperson
The X9F6 working group that revised this standard consisted of the following members:

John Sheets, Chairperson

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACI Worldwide</td>
<td>Doug Grote</td>
</tr>
<tr>
<td>ACI Worldwide</td>
<td>Dan Kinney</td>
</tr>
<tr>
<td>Apriva</td>
<td>Len Sutton</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Andi Coleman</td>
</tr>
<tr>
<td>DeLap LLP</td>
<td>Darlene Kargel</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Bruce Chapa</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Anne Konecny</td>
</tr>
<tr>
<td>Dresser Wayne</td>
<td>Tim Weston</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Andrea Beatty</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Lisa Curry</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Lilik Kazaryan</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Dan Otten</td>
</tr>
<tr>
<td>Futurex</td>
<td>Chris Hamlett</td>
</tr>
<tr>
<td>GEOBRIDGE Corporation</td>
<td>Jason Way</td>
</tr>
<tr>
<td>Gilbarco</td>
<td>Bruce Welch</td>
</tr>
<tr>
<td>Heartland Payment Systems</td>
<td>Sarah McCrarry</td>
</tr>
<tr>
<td>Heartland Payment Systems</td>
<td>Glenda Preen</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>Larry Hines</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>Susan Langford</td>
</tr>
<tr>
<td>Hypercom</td>
<td>Mohammad Arif</td>
</tr>
<tr>
<td>Hypercom</td>
<td>LeAnn Brown</td>
</tr>
<tr>
<td>Hypercom</td>
<td>Gary Zempich</td>
</tr>
<tr>
<td>IBM Corporation</td>
<td>Todd Arnold</td>
</tr>
<tr>
<td>Ingenico</td>
<td>John Spence</td>
</tr>
<tr>
<td>J.P. Morgan Chase &amp; Co</td>
<td>Donna Meagher</td>
</tr>
<tr>
<td>K3DES LLC</td>
<td>Azie Amini</td>
</tr>
<tr>
<td>K3DES LLC</td>
<td>James Richardson</td>
</tr>
<tr>
<td>Keely Consulting</td>
<td>Martha Keely</td>
</tr>
<tr>
<td>Key Innovations</td>
<td>Scott Spiker</td>
</tr>
<tr>
<td>MagTek, Inc.</td>
<td>Larry Meyers</td>
</tr>
<tr>
<td>Merchant Advisory Group</td>
<td>Brad Andrews</td>
</tr>
<tr>
<td>Merchant Advisory Group</td>
<td>Dodd Roberts</td>
</tr>
<tr>
<td>Mustang Microsystems, Inc.</td>
<td>Tom Galloway</td>
</tr>
</tbody>
</table>
This is the second release of this document. A new key derivation method has been added. Key types and usages have also been clarified.

This document is to be used in conjunction with implementation of ANS X9.8 and ANS X9.24 Part 1.
Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

1 Scope

This document describes a method consistent with the requirements of ANS X9.24 Retail Financial Services Symmetric Key Management Part 1 for the secure exchange of keys and other sensitive data between two devices that share a symmetric key exchange key. This method may also be used for the storage of keys under a symmetric key.

This document is not a security standard and is not intended to establish security requirements. It is intended instead to provide an interoperable method of implementing security requirements and policies.

2 References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2. ANS X9.24 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys; (draft)
3. ANS X3.92 Data Encryption Algorithm (DEA)