American National Standard for Financial Services

ANSI X9.24-3-2017

Retail Financial Services

Symmetric Key Management

Part 3: Derived Unique Key Per Transaction

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: October 11, 2017

American National Standards Institute

This page intentionally left blank

Contents Page

Figures vi
Tables vii
Foreword viii
Introduction ix
1 Purpose 1
2 Scope 1
2.1 Application 1
3 Normative references 2
4 Terms and definitions 3
4.1 Advanced Encryption Standard (AES) 3
4.2 AES 3
4.3 algorithm 3
4.4 ANSI 3
4.5 base derivation key (BDK) 3
4.6 BDK 3
4.7 BDK ID 3
4.8 cryptographic key 3
4.9 cryptographic key synchronization 4
4.10 cryptographic strength 4
4.11 derivation 4
4.12 derivation identifier (ID) 4
4.13 derivation key 4
4.14 Derived Unique Key Per Transaction (DUKPT) 4
4.15 Initial DUKPT key 4
4.16 Initial Key 4
4.17 Initial Key ID 5
4.18 ISO 5
4.19 key 5
4.20 PAN 5
4.21 Personal Identification Number (PIN) 5
4.22 Primary Account Number (PAN) 5
4.23 PIN 5
4.24 Secure Cryptographic Device (SCD) 5
4.25 SCD 5
4.26 symmetric key 6
4.27 TDEA 6
4.28 Transaction-Originating SCD 6
4.29 Triple Data Encryption Algorithm (TDEA) 6
4.30 Working Key 6
5 Overview 6
5.1 Key Management 6
5.2 Cryptographic Key Synchronization 9
5.3 Unique Initial Keys 9
6 AES DUKPT 10
6.1 Algorithm Description 11
6.1.1 KSN Compatibility Mode 14

6.1.2 Derived Key OIDs 15
6.1.3 Keys and Key Sizes 15
6.2.2 Key Length Function 16
6.3 Key Derivation Function 16
6.3.1 Algorithm 16
6.3.2 Derivation Data 18
6.3.3 “Create Derivation Data” (Local Subroutine) 21
6.3.4 Security Considerations 22
6.4 Host Security Module Algorithm 23
6.5 Transaction-Originating Device Algorithm 27
6.5.1 Algorithm Parameters 27
6.5.2 Storage Areas 27
6.5.3 Processing Routines 28
6.5.4 Base Cipher Definitions 32

Annex A. Annex A (Informative) Pseudocode Notation 34

Annex B. Annex B (Informative) Test Vectors 37

Annex C. Annex C (Informative) TDEA Derived Unique Key per Transaction 42

Figures

Figure 1 - DUKPT at Receiving SCD 8
Figure 2 - DUKPT at Originating SCD 9
Figure 3 - KDF in Counter Mode 17
Figure 4 - Simplified DUKPT Data Flow 50
Figure 5 - Key Calculation for PIN Encrypting Key and MAC Keys 54
Figure 6 - Key Calculation for Data Encryption Keys 55
Figure 7 - 2 Key Triple DEA Initial Key 65

Tables

Table 1 - AES DUKPT allowed working keys per BDK size 15
Table 2 - Terminal Key Derivation Data 18
Table 3 - Other Key Derivation Data 19
Table 4 - BDK and Associated Data for Test Vectors 37
Table 4 - Variant Constants for Transaction Keys 55

Foreword

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 interpretation 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, Incorporated
Financial Industry Standards
275 West Street Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

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

By publication of this standard, 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 nondiscriminatory 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 Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 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.

The X9 committee had the following members:

Roy C. DeCicco, X9 Chair
Angela Hendershott, X9 Vice Chair
Steve Stevens, X9 Executive Director
Janet Busch, Program Manager

Organization Represented	***Representative***
ACI Worldwide	Doug Grote
American Bankers Association	Diane Poole
American Express Company	David Moore
Bank of America	Daniel Welch
Bank of New York Mellon	Arthur Sutton
Blackhawk Network	Anthony Redondo
Bloomberg LP	Corby Dear
Capital One	Marie LaQuerre
Citigroup, Inc.	Karla McKenna
CLS Bank	Ram Komarraju
Conexxus, Inc.	Gray Taylor
CUSIP Service Bureau	Gerard Faulkner
Delap LLP	Andrea Beatty
Delap LLP	Darlene Kargel
Deluxe Corporation	Angela Hendershott
Diebold Nixdorf	Bruce Chapa
Discover Financial Services	Michelle Zhang
eCurrency	David Wen
Federal Reserve Bank	Mary Hughes
First Data Corporation	Lisa Curry
FIS	Stephen Gibson-Saxty
Fiserv	Dan Otten