# American National Standard for Financial Services

# ANS X9.24 Part 2: 2016

# Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

Secretariat

**Accredited Standards Committee X9, Incorporated**

**Financial Industry Standards**

Date Approved: November 25, 2016

**American National Standards Institute**

# 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**CAUTION NOTICE:** This American National Standard may be revised or withdrawn at any time.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 21403 USA**
**X9 Online http://www.x9.org**

# Contents


Foreword ..... i

Figures ..... iv

Tables ..... v

Introduction ..... vi

1 Purpose ..... 13

2 Scope ..... 14
2.1 Application ..... 14

3 References ..... 14

4 Terms and Definitions ..... 15

5 Standard Organization ..... 21

6 Environment ..... 22
6.1 General ..... 22
6.2 Cardholder and Card Issuer ..... 23
6.3 Card Acceptor ..... 24
6.4 Acquirer ..... 24
6.5 Secure Cryptographic Device (SCD) ..... 24
6.6 Acquirer Host ..... 25
6.7 Certification Authority ..... 25
6.8 Device Manufacturer ..... 25

7 Key Management Requirements ..... 25
7.1 General ..... 25
7.1.1 Symmetric Keys ..... 25
7.1.2 Asymmetric Keys ..... 26
7.2 Secure Cryptographic Devices (SCD) used for Key Management ..... 27
7.3 A Secure Environment ..... 27
7.4 Certification Authority (CA) Requirements ..... 27
7.5 Registration Authority (RA) Requirements ..... 28
7.6 Key Generation ..... 29
7.6.1 Symmetric Key Generation ..... 29
7.6.2 Asymmetric Key Generation ..... 29
7.7 Asymmetric Key Activation/Enablement ..... 29
7.7.1 Creation of Certificates ..... 29
7.7.2 Signing of Certificates ..... 30
7.7.3 Lifetime of Certificates ..... 30
7.7.4 Authentication of Valid Request and Valid Device ..... 30
7.8 Key Distribution ..... 30
7.8.1 Symmetric Key Distribution ..... 30
7.8.2 Asymmetric Key Distribution ..... 31
7.9 Key Utilization ..... 32
7.9.1 Symmetric Key Utilization ..... 32
7.9.2 Asymmetric Key Utilization ..... 32
7.10 Key Storage ..... 33
7.11 Key Replacement ..... 33

**7.12 Key Destruction ..... 33**

**8 Trust Models and Key Establishment Protocols ..... 34**
**8.1 Introduction ..... 34**
**8.2 Trust Models ..... 34**
**8.2.1 Three-Party Model – Third Party CA ..... 34**
**8.2.2 Two-Party Model – One Party Acts as CA ..... 35**
**8.2.3 Prior Trust Model – No CA ..... 38**
**8.3 Symmetric Key Establishment Protocols ..... 38**
**8.3.1 Unilateral Key Transport Method ..... 38**
**8.3.2 Bilateral Key Transport Method (Both Parties Generate and Share Symmetric Key – Joint Control) ..... 39**
**8.3.3 Key Agreement Method ..... 41**

**Annex A (Normative)** Approved ANSI Symmetric Key Algorithms for Encryption of Private Keys ..... **44**

# Figures

**Figure 1,** Example of Hierarchical Trust Domain/Sub-Domains .....23

Figure 2 Three Party Example: Key Distribution to KRDs .....35

Figure 3 Two Party Example: Key distribution to KRDs; manufacturer of KRDs plays role of CA .....36

Figure 4 Two Party Example: Key distribution to KRDs; KDH plays role of CA.....37

Figure 5 Two Party Example: Key distribution between interchange nodes.....37

Figure 6 High Level Overview of Key Transport Method (Unilateral) .....38

Figure 7 High Level Overview of Key Transport Method (Bilateral).....40

Figure 8 High Level Overview of Key Agreement Method .....41

# Tables

Table 1 Trust Models and Key Establishment Protocols ..... 34

# Introduction

Today, billions of dollars in funds are transferred electronically by various communication methods. Transactions are often entered remotely, off-premise from financial institutions, by retailers or by customers directly. Such transactions are transmitted over potentially non-secure media. The vast range in value, size, and the volume of such transactions expose institutions to severe risks, which may be uninsurable.

To protect these financial messages and other sensitive information, many institutions are making use of the American National Standards Institute Triple Data Encryption Algorithm (TDEA), or the algorithm defined in the Advanced Encryption Standard (AES). Specific examples of TDEA use include standards for message authentication, personal identification number encryption, other data encryption, and key encryption.

The TDEA and AES are in the public domain. The security and reliability of any process based on these algorithms is directly dependent on the protection afforded to secret numbers called cryptographic keys.

A familiar analogy may be found in the combination lock of a vault. The lock design is public knowledge. Security is provided by keeping a number, the combination, a secret. Secure operation also depends on protective procedures and features which prevent surreptitious viewing or determination of the combination by listening to its operation. Procedures are also required to ensure that the combination is random and cannot be modified by an unauthorized individual without detection.

**Part 1 of ANS X9.24 deals exclusively with management of symmetric keys using symmetric techniques. This Part 2 addresses the use of asymmetric techniques for the distribution of symmetric keys. Asymmetric techniques utilize algorithms other than the DEA (e.g., Diffie-Hellman, RSA, Elliptic Curve, etc.). Those asymmetric algorithms are defined in other American National Standards Institute standards (e.g., ANS X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Algorithm Keys Using Discrete Logarithm Cryptography, ANS X9.44 DRAFT Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Factoring-Based Cryptography, and X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Management Using Elliptic Curve-Based Cryptography). Those algorithms are also in the public domain, and the security and reliability are also dependent on the security and integrity of the asymmetric keys and the infrastructure under which those keys are created and managed.**

**This part of ANS X9.24 assumes the reader is familiar with the concepts behind asymmetric cryptography.**

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 of this standard will be welcome. They should be sent to the ASC X9 Secretariat, Accredited Standards Committee X9, Inc., 275 West Street, Suite 107 Annapolis, MD 21403.

The standard was processed and approved for submittal to the American National Standards Institute by the Accredited Standards Committee X9 - Financial Services. Committee approval of the standard does not

necessarily imply that all committee members voted for its approval. At the time it approved this standard, the X9 Committee had the following members:

Roy C. DeCicco, X9 Chairman
Claudia Swendseid, X9 Vice Chairman
Steve Stevens, Executive Director
Janet Busch, Program Director

| ***Organization Represented*** | ***Representative*** |
|---|---|
| All My Papers | Larry Krummel |
| ACI Worldwide | Doug Grote |
| ACI Worldwide | Dan Kinney |
| American Bankers Association | Diane Poole |
| American Express Company | David Moore |
| Bank of America | Daniel Welch |
| Bank of New York Mellon | Bryan Kirkpatrick |
| BlackBerry Limited | Daniel Brown |
| Blackhawk Network | Anthony Redondo |
| Bloomberg LP | Corby Dear |
| Capital One | Marie LaQuerre |
| Citigroup, Inc. | Karla McKenna |
| CLS Bank | Ram Komarraju |
| Conexxus, Inc. | Michael Davis |
| Conexxus, Inc. | Gray Taylor |
| Delap LLP | Darlene Kargel |
| Deluxe Corporation | Angela Hendershott |
| Diebold, Inc. | Bruce Chapa |
| Discover Financial Services | Michelle Zhang |
| eCurrency | David Wen |
| Federal Reserve Bank | Mary Hughes |
| Federal Reserve Bank | Janet LaFrence |
| Federal Reserve Bank | Claudia Swendseid |
| FIS | Stephen Gibson-Saxty |
| Fiserv | Dan Otten |
| FIX Protocol Ltd - FPL | Jim Northey |
| Futurex | Ryan Smith |
| Gilbarco | Bruce Welch |
| Harland Clarke | John McCleary |
| Hewlett Packard | Susan Langford |
| IBM Corporation | Todd Arnold |
| Independent Community Bankers of America | Cary Whaley |
| Ingenico | Rob Martin |
| ISITC | Jason Brasile |
| J.P. Morgan Chase | Roy DeCicco |
| KPMG LLP | Mark Lundin |
| MagTek, Inc. | Roger Applewhite |
| MagTek, Inc. | Mimi Hart |
| MasterCard Europe Sprl | Mark Kamers |
| NACHA The Electronic Payments Association | Priscilla Holland |
| National Security Agency | Paul Timmel |
| NCR Corporation | David Norris |
| Office of Financial Research, U.S. Treasury Department | Justin Stekervetz |
| PCI Security Standards Council | Troy Leach |
| RouteOne | Chris Irving |
| RouteOne | Jenna Wolfe |

State Street Corporation ..... Sharon Cournoyer
SWIFT/Pan Americas ..... Frank Vandriessche
Symcor Inc. ..... Debbi Fitzpatrick
TECSEC Incorporated ..... Ed Scheidt
The Clearing House ..... Sharon Jablon
U.S. Bank ..... John King
U.S. Commodity Futures Trading Commission (CFTC) ..... Robert Stowsky
USDA Food and Nutrition Service ..... Kathy Ottobre
Vantiv LLC ..... Gary Zempich
VeriFone, Inc. ..... Dave Faoro
VISA ..... Kim Wagner
Wayne Fueling Systems ..... Steven Bowles
Wells Fargo Bank ..... Mark Schaffer

At the time it approved this standard, the X9F Subcommittee on Data and Information Security had the following members:

Dave Faoro, Chairperson

| ***Organization Represented*** | ***Representative*** |
|---|---|
| ACI Worldwide | Richard DuVall |
| ACI Worldwide | Doug Grote |
| ACI Worldwide | Dan Kinney |
| ACI Worldwide | Julie Samson |
| American Bankers Association | Tom Judd |
| American Express Company | David Armes |
| American Express Company | Eric Eldridge |
| American Express Company | William J. Gray |
| American Express Company | Farid Hatefi |
| American Express Company | Vicky Sammons |
| American Express Company | John Timar |
| Bank of America | Amanda Adams |
| Bank of America | Peter Capraro |
| Bank of America | Andi Coleman |
| Bank of America | Lawrence LaBella |
| Bank of America | Will Robinson |
| Bank of America | Michael Smith |
| Bank of America | Daniel Welch |
| BlackBerry Limited | Daniel Brown |
| BlackBerry Limited | Sandra Lambert |
| Blackhawk Network | Anthony Redondo |
| Bloomberg LP | Erik Anderson |
| Bloomberg LP | Corby Dear |
| Capital One | Marie LaQuerre |
| Capital One | Johnny Lee |
| Cipherithm | Scott Spiker |
| comForte 21 GmbH | Thomas Gloerfeld |
| comForte 21 GmbH | Henning Horst |
| Communications Security Establishment | Jonathan Hammell |
| Communications Security Establishment | David Smith |
| Conexxus, Inc. | Alan Thiemann |
| CUSIP Service Bureau | Scott Preiss |
| Delap LLP | David Buchanan |

| | |
|---|---|
| Delap LLP | Darlene Kargel |
| Deluxe Corporation | Angela Hendershott |
| Deluxe Corporation | Margiore Romay |
| Deluxe Corporation | Andy Vo |
| Diebold, Inc. | Bruce Chapa |
| Diebold, Inc. | Michael Ott |
| Diebold, Inc. | Dave Phister |
| Discover Financial Services | Cheryl Mish |
| Discover Financial Services | Diana Pauliks |
| Discover Financial Services | Jordan Schaefer |
| eCurrency | David Wen |
| Federal Reserve Bank | Patrick Adler |
| Federal Reserve Bank | Cynthia Baxter |
| Federal Reserve Bank | Guy Berg |
| Federal Reserve Bank | Julia Cheney |
| Federal Reserve Bank | Marianne Crowe |
| Federal Reserve Bank | Sandeep Dhameja |
| Federal Reserve Bank | Amanda Dorphy |
| Federal Reserve Bank | Mary Hughes |
| Federal Reserve Bank | Heather Hultquist |
| Federal Reserve Bank | Janet LaFrence |
| Federal Reserve Bank | Jackie Nugent |
| Federal Reserve Bank | Jim O'Connell |
| Federal Reserve Bank | Susan Pandy |
| Federal Reserve Bank | Patti Ritter |
| Federal Reserve Bank | Daniel Rozycki |
| Federal Reserve Bank | Rick Sullivan |
| Federal Reserve Bank | Claudia Swendseid |
| First Data Corporation | Andrea Beatty |
| First Data Corporation | Lisa Curry |
| First National Bank of Omaha | Kristi White |
| Fiserv | Bud Beattie |
| Fiserv | Dan Otten |
| Futurex | Ryan Smith |
| GEOBRIDGE Corporation | Donna Gem |
| GEOBRIDGE Corporation | Jason Way |
| Gilbarco | Bruce Welch |
| Harland Clarke | Joseph Filer |
| Heartland Payment Systems | Scott Meeker |
| Hewlett Packard | Susan Langford |
| Hewlett Packard | Terence Spies |
| IBM Corporation | Todd Arnold |
| Independent Community Bankers of America | Cary Whaley |
| Ingenico | Rob Martin |
| ITS, Inc. (SHAZAM Networks) | Manish Nathwani |
| J.P. Morgan Chase | Bruce Geller |
| J.P. Morgan Chase | Kathleen Krupa |
| J.P. Morgan Chase | Jackie Pagán |
| K3DES LLC | Azie Amini |
| KPMG LLP | Mark Lundin |
| MagTek, Inc. | Jeff Duncan |
| MagTek, Inc. | Mimi Hart |
| MasterCard Europe Sprl | Mark Kamers |
| MasterCard Europe Sprl | Joshua Knopp |
| MasterCard Europe Sprl | Larry Newell |
| MasterCard Europe Sprl | Adam Sommer |

| | |
|---|---|
| MasterCard Europe Sprl | Michael Ward |
| National Institute of Standards and Technology (NIST) | Elaine Barker |
| National Institute of Standards and Technology (NIST) | Lily Chen |
| National Security Agency | Mike Boyle |
| National Security Agency | Paul Timmel |
| NCR Corporation | Charlie Harrow |
| NCR Corporation | David Norris |
| PCI Security Standards Council | Leon Fell |
| PCI Security Standards Council | Troy Leach |
| PCI Security Standards Council | Ralph Poore |
| Richard Sweeney | Richard Sweeney |
| RSA, The Security Division of EMC | Steve Schmalz |
| SafeNet, Inc. | Amit Sinha |
| Security Innovation | Mark Etzel |
| Security Innovation | William Whyte |
| Security Innovation | Lee Wilson |
| Security Innovation | Zhenfei Zhang |
| TECSEC Incorporated | Ed Scheidt |
| TECSEC Incorporated | Dr. Wai Tsang |
| TECSEC Incorporated | Jay Wack |
| Thales UK Limited | Larry Hines |
| Thales UK Limited | James Torjussen |
| The Clearing House | Henry Farrar |
| Trustwave | John Amaral |
| Trustwave | Tim Hollebeek |
| U.S. Bank | Stephen Case |
| U.S. Bank | Peter Skirvin |
| Vantiv LLC | Dick Bloss |
| Vantiv LLC | Tom Humphrey |
| Vantiv LLC | Scott Mackelprang |
| Vantiv LLC | Bill Weingart |
| Vantiv LLC | Gary Zempich |
| Vantiv LLC | James Zerfas |
| VeriFone, Inc. | John Barrowman |
| VeriFone, Inc. | David Ezell |
| VeriFone, Inc. | Dave Faoro |
| VeriFone, Inc. | Doug Manchester |
| VeriFone, Inc. | Brad McGuinness |
| VeriFone, Inc. | Joachim Vance |
| VISA | Shahzad Khan |
| VISA | Kim Wagner |
| Wayne Fueling Systems | Steven Bowles |
| Wells Fargo Bank | William Felts, IV |
| Wells Fargo Bank | Phillip Griffin |
| Wells Fargo Bank | Jan Kohl |
| Wells Fargo Bank | Garrett Macey |
| Wells Fargo Bank | Mike McCormick |
| Wells Fargo Bank | Mark Schaffer |
| Wells Fargo Bank | Jeff Stapleton |
| Wincor Nixdorf Inc | Christoph Bruecher |
| Wincor Nixdorf Inc | Andrea Carozzi |
| Wincor Nixdorf Inc | Michael Nolte |
| XYPRO Technology | Steve Tcherchian |

The X9F6 working group that wrote this standard consisted of the following members:

Scott Spiker, Chairperson
Darlene Kargel, Vice Chairperson

| *Organization Represented* | *Representative* |
|---|---|
| ACI Worldwide | Dan Kinney |
| ACI Worldwide | Julie Samson |
| American Express Company | Alan Fong |
| American Express Company | Michael Hyzer |
| Bank of America | Andi Coleman |
| Cipherithm | Scott Spiker |
| comForte 21 GmbH | Henning Horst |
| Conexxus, Inc. | Alan Thiemann |
| Conexxus, Inc. | Linda Toth |
| Delap LLP | David Buchanan |
| Delap LLP | Darlene Kargel |
| Diebold, Inc. | Bruce Chapa |
| Diebold, Inc. | Anne Konecny |
| Discover Financial Services | Diana Pauliks |
| Federal Reserve Bank | Amanda Dorphy |
| First Data Corporation | Andrea Beatty |
| First Data Corporation | Lisa Curry |
| First Data Corporation | Randall Rieth |
| Fiserv | Dan Otten |
| Futurex | Chris Hamlett |
| Futurex | Ryan Smith |
| GEOBRIDGE Corporation | Donna Gem |
| GEOBRIDGE Corporation | Dean Macinskas |
| GEOBRIDGE Corporation | Jason Way |
| Gilbarco | Bruce Welch |
| Heartland Payment Systems | Randy Ison |
| Heartland Payment Systems | John Masden |
| Hewlett Packard | Susan Langford |
| IBM Corporation | Todd Arnold |
| Ingenico | Rob Martin |
| Ingenico | Steve McKibben |
| J.P. Morgan Chase | Kathleen Krupa |
| J.P. Morgan Chase | Darryl Scott |
| K3DES LLC | Azie Amini |
| K3DES LLC | James Richardson |
| Mainsail Trim, Inc. | Norman Cecil |
| NCR Corporation | Charlie Harrow |
| PCI Security Standards Council | Ralph Poore |
| Thales UK Limited | Colette Broadway |
| Thales UK Limited | Larry Hines |
| Thales UK Limited | James Torjussen |
| Trustwave | Tim Hollebeek |
| U.S. Bank | Stephen Case |
| Vantiv LLC | Gary Zempich |
| Vantiv LLC | James Zerfas |
| VeriFone, Inc. | Dave Faoro |
| VeriFone, Inc. | Doug Manchester |
| VeriFone, Inc. | Joachim Vance |
| VISA | Adam Clark |
| VISA | Shahzad Khan |

VISA.....Michael Stefanich
VISA.....Kim Wagner
Wayne Fueling Systems.....Steven Bowles
Wells Fargo Bank.....Jeff Jacoby
XYPRO Technology.....Steve Tcherchian

Special thanks to Charlie Harrow of NCR Corporation, the technical editor of this standard.

# Retail Financial Services
# Symmetric Key Management
# Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

## 1 Purpose

The financial services industry desires an additional and cost effective method of implementing symmetric key distribution at remote devices and between communicating pairs. Compliant implementation of the requirements stated in ANS X9.24 Part 1 for the secure management of symmetric keys requires (among other things) unique keys per device and strict enforcement of dual control and split knowledge processes for handling the full-length (i.e., not concatenated) keying material deployed to remote devices or established between communicating pairs. Historically, *compliant* implementation of key distribution has been a manually performed, physically on-site process that is difficult to manage, costly, and/or non-existent (i.e., not compliant). An automated rather than manual method of distributing symmetric keys could address these issues and could result in improved security of the financial services networked environment.

The use of public key cryptography and associated asymmetric key algorithms is one proposed solution for automated remote symmetric key distribution. Unlike clear symmetric keys which are to be protected from disclosure at all times during their key life cycle, the clear public keys of the asymmetric key pairs may be exchanged over open networks. This characteristic allows for automated distribution from a remote location and may eliminate the above issues associated with manual key loading. Once distributed, the protocols associated with the asymmetric algorithms may be used to establish the symmetric key, and may eliminate the manual symmetric key loading process and its associated risks. There are two such protocols for establishing the symmetric key. The key transport protocol may be used by the sender to encrypt and transport the symmetric key to the receiver. The key agreement protocol may be used to mutually derive the symmetric key.

The security and reliability of any process based on public key algorithms is directly dependent on the protection afforded to the secrecy of each key pair's associated private key and the integrity of the key pair and Public Key Infrastructure (PKI) environment under which those key pairs are created and managed. Key modulus sizes and the underlying mathematics of the asymmetric key algorithms should also be considered as factors in the overall security of the implementation. The public key validation is a very important security aspect. Implementation of the system includes measures to prevent man-in-the-middle attacks on the system, and ensure the mutual authentication of the sender and receiver of the keys.

This part of ANS X9.24 establishes requirements and guidelines for the secure management and application-level interoperability of such automated keying operations. This part of this standard addresses symmetric keys managed with asymmetric keys, and asymmetric keys managed with symmetric keys (as in the storage of private keys encrypted with a symmetric master key for storage as cryptograms on a local database). This part of ANS X9.24 does NOT address using asymmetric keys to encrypt the Personal Identification Number (PIN) and does NOT address asymmetric keys managed with asymmetric keys.

## 2 Scope

This part of ANS X9.24 covers the establishment of device initial trust and management of keying material used for financial services such as point of sale (POS) transactions, automatic teller machine (ATM) transactions, messages among terminals and financial institutions, and interchange messages among acquirers, switches and