American National Standard
for Financial Services

ANSI X9.24 Part 2: 2021

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: September 30, 2021

American National Standards Institute

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., 275 West Street, Suite 107, Annapolis, MD 21401.

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CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time.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

Copyright © 2021 Accredited Standards Committee 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. Printed in the United States of America.

Contents

Foreword i
Figures iv
Tables v
Introduction vi
1 Purpose 15
2 Scope 15
2.1 Application 16
3 References 16
3.1 Normative References 16
3.2 Informative References 17
4 Terms and Definitions 18
5 Standard Organization 24
6 Environment 25
6.1 General 25
6.2 Cardholder and Card Issuer 26
6.3 Card Acceptor 27
6.4 Acquirer 27
6.5 Secure Cryptographic Device (SCD) 27
6.6 Acquirer Host 28
6.7 Certification Authority 28
6.8 Device Manufacturer 28
7 Key Management Requirements 28
7.1 General 28
7.1.1 Symmetric Keys 28
7.1.2 Asymmetric Keys 29
7.2 Secure Cryptographic Devices (SCD) used for Key Management 30
7.3 A Secure Environment 30
7.4 Certification Authority (CA) Requirements 31
7.5 Registration Authority (RA) Requirements 31
7.6 Key Generation 32
7.6.1 Symmetric Key Generation 32
7.6.2 Asymmetric Key Generation 32
7.7 Asymmetric Key Activation/Enablement 33
7.7.1 Creation of Certificates 33
7.7.2 Signing of Certificates 33
7.7.3 Lifetime of Certificates 33
7.7.4 Authentication of Valid Request and Valid Device 33
7.8 Key Distribution 34
7.8.1 Symmetric Key Distribution 34
7.8.2 Asymmetric Key Distribution 34
7.9 Key Utilization 37
7.9.1 Symmetric Key Utilization 37
7.9.2 Asymmetric Key Utilization 37
7.10 Key Storage 37

© 2021 – All rights reserved

7.11 Key Replacement 37
7.12 Key Destruction 38

8 Trust Models and Key Establishment Protocols 38
8.1 Introduction 38
8.2 Trust Models 39
Mechanisms SHALL exist to establish trust for all public keys used in the key exchange and key transport protocols 39
8.2.1 Three-Party Model – Third Party CA 39
8.2.2 Two-Party Model – One Party Acts as CA 40
8.2.3 Prior Trust Model – No CA 42
8.3 Symmetric Key Establishment Protocols 43
8.3.1 Unilateral Key Transport Method 43
8.3.2 Bilateral Key Transport Method (Both Parties Generate and Share Symmetric Key – Joint Control) 44
8.3.3 Key Agreement Method 45

Annex A (Informative) Encrypting an Asymmetric Key Pair Using Asymmetric Techniques 47

Annex B (Informative) Examples of Certificate Authority Topologies 51

© 2021 – All rights reserved

Figures

Figure 1, Example of Hierarchical Trust Domain/Sub-Domains....26

Figure 2 Three Party Example: Key Distribution to KRDs....40

Figure 3 Two Party Example: Key distribution to KRDs; manufacturer of KRDs plays role of CA....41

Figure 4 Two Party Example: Key distribution to KRDs; KDH plays role of CA....41

Figure 5 Two Party Example: Key distribution between interchange nodes....42

Figure 6 High Level Overview of Key Transport Method (Unilateral)....43

Figure 7 High Level Overview of Key Transport Method (Bilateral)....44

Figure 8 High Level Overview of Key Agreement Method....46

Figure 9- Encrypting an Asymmetric Key Pair using Public Key Techniques and a Symmetric Ephemeral Key....47

Figure 10- Encrypting an Asymmetric Key Pair using Diffie-Hellman Techniques and a Derived Symmetric Ephemeral Key....48

© 2021 – All rights reserved

Tables

Table 1 Recording of Private Key Operations 30

Table 2 Trust Models and Key Establishment Protocols 39

© 2021 – All rights reserved

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.

The Financial Services industry is migrating to AES. References to TDEA in this standard are included for backward compatibility but a sunset date may be announced prior to the release of the next version of this standard. New applications should use AES. Migration away from TDEA is currently recommended. TDEA should not be used for new implementations.

As this standard is focused on the delivery of keys using asymmetric techniques, the impact to users of this standard includes ensuring the keys used to distribute AES keys are of sufficient strength. To enable delivery of AES keys larger than 128 bits, Elliptic Curve should be considered as an alternative to RSA.

It should also be noted that large-scale Quantum Computers are a threat to the security of asymmetric algorithms. New Post Quantum Cryptography methods are being investigated and vetted for use within the Financial Services industry. At the time of publication of this version of this standard, the methods remain undecided. Migration considerations and impacts related to the sunset of TDEA should include the concept of creating crypto-agility within your environment to enable adoption of new algorithms. It should be assumed that any key protected by asymmetric techniques will need to be changed for security, if a large-scale Quantum

© 2021 – All rights reserved

Computer becomes a reality. For further information, see ASCX9 IR 01-2019, Quantum Computing Risks to the Financial Services Industry.

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 21401.

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:

Corby Dear, X9 Chairman
Steve Stevens, Executive Director
Janet Busch, Program Director
Ambria Frazier, Program Manager

Organization Represented	***Representative***
Amazon	Igor Kleyman
American Bankers Association	Tab Stewart
Bank of America	Daniel Welch
BDO	Tim Crawford
Bloomberg LP	Corby Dear
Conexxus, Inc.	Alan Thiemann
CUSIP Global Services	Gerard Faulkner
Delap LLP	Andrea Beatty
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Bruce Chapa
Digicert	Dean Coclin
Dover Fueling Solutions	Henry Fieglein
Federal Reserve Bank	Ainsley Hargest
FirstBank	Ryan Buerger
FIS	Stephen Gibson-Saxty
Fiserv	Lisa Curry
Fiserv	Dan Otten
FIX Protocol Ltd - FPL	James Northey
Futurex	Ryan Smith
Gilbarco	Bruce Welch
Harland Clarke	Jonathan Lee
Hyosung TNS Inc.	Joe Militello
IBM Corporation	Richard Kisley
Ingenico	Steven Bowles
ISITC	Lisa Iagatta
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Ted Rothschild
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
NACHA The Electronic Payments Association	George Throckmorton

© 2021 – All rights reserved

National Security Agency	Mike Boyle
NCR Corporation	Charlie Harrow
Office of Financial Research, U.S. Treasury Department	Thomas Brown Jr.
PCI Security Standards Council	Troy Leach
SWIFT/Pan Americas	Anne Suprenant
TECSEC Incorporated	Ed Scheidt
The Clearing House	Sharon Jablon
U.S. Bank	Michelle Wright
U.S. Commodity Futures Trading Commission (CFTC)	Robert Stowsky
University Bank	Stephen Ranzini
USDA Food and Nutrition Service	Lisa Gifaldi
VeriFone, Inc.	Joachim Vance
Viewpointe	Richard Luchak
VISA	Kristina Breen
Wells Fargo Bank	Sotos Barkas
Zions Bank	Kay Hall

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

Steven Bowles, Chairperson
Ed Scheidt, Vice Chairperson

Organization Represented	***Representative***
ACI Worldwide	Dan Kinney
ACI Worldwide	Julie Samson
Amazon	Sean Estrada
Amazon	Sandra Lambert
American Express Company	Gail Chapman
American Express Company	Farid Hatefi
American Express Company	Peter Markall
American Express Company	John Timar
American Express Company	Kevin Welsh
Bank of America	Amanda Adams
Bank of America	Andi Coleman
Bank of America	Joel Kazin
Bank of America	Terry McKinney
Bank of America	Matt Sharp
Bank of America	Michael Smith
Bank of America	Daniel Welch
BBVA Compass	Omar Jarrar
BDO	Tim Crawford
Bloomberg LP	Erik Anderson
Bloomberg LP	Corby Dear
Capital One	Johnny Lee
comforte AG	Thomas Gloerfeld
comforte AG	Henning Horst
Communications Security Establishment	Jonathan Hammell
Conexxus, Inc.	David Ezell
Conexxus, Inc.	Alan Thiemann
CUSIP Global Services	Scott Preiss
Delap LLP	Andrea Beatty
Delap LLP	Diane Bishop

© 2021 – All rights reserved

Delap LLP	David Buchanan
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	David Phister
Digicert	Tim Hollebeek
Discover Financial Services	Susan Pandy
Discover Financial Services	Jordan Schaefer
Discover Financial Services	Jorge Vargas
Dover Fueling Solutions	Henry Fieglein
Federal Reserve Bank	Guy Berg
Federal Reserve Bank	Marianne Crowe
Federal Reserve Bank	Ken Han
Federal Reserve Bank	Ainsley Hargest
Federal Reserve Bank	Daniel Maynard
Federal Reserve Bank	Patti Ritter
First National Bank of Omaha	Robert Lamagna-Reiter
First National Bank of Omaha	Sherry Rewolinski
First National Bank of Omaha	Kristi White
Fiserv	Bud Beattie
Fiserv	Lisa Curry
Fiserv	Vinayak Kagalkar
Fiserv	Dan Otten
Futurex	Comron Moeni
Futurex	Ryan Smith
Futurex	Tim Weston
GEOBRIDGE Corporation	Jason Way
Gilbarco	Scott Turner
Gilbarco	Bruce Welch
Harland Clarke	Joseph Filer
Hyosung TNS Inc.	Joe Militello
Hyosung TNS Inc.	JaeWhan Shin
IBM Corporation	Richard Kisley
Ingenico	Steven Bowles
Ingram Micro	Candice Hoft
ISARA Corporation	Mike Brown
ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Darryl Scott
K3DES LLC	Mukul Gupta
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Mark Kamers
MasterCard Europe Sprl	Michael Ward
Member Emeritus	Larry Hines
Micro Focus LLC - USSM	John Ivie
Micro Focus LLC - USSM	Luther Martin
Micro Focus LLC - USSM	Timothy Roake
Micro Focus LLC - USSM	Phil Smith III
Microsoft	Paul Adare
Microsoft	Mike Reilly
National Institute of Standards and Technology (NIST)	Elaine Barker
National Institute of Standards and Technology (NIST)	Lily Chen
National Security Agency	Mike Boyle

© 2021 – All rights reserved

National Security Agency	Nick Gajcowski
National Security Agency	Paul Timmel
NCR Corporation	Charlie Harrow
NCR Corporation	Bradford Loewy
P97 Networks, Inc.	Steve Moses
PCI Security Standards Council	Leon Fell
PCI Security Standards Council	Troy Leach
PCI Security Standards Council	Ralph Poore
PCI Security Standards Council	Joel Weisz
SteinTech LLC	Clay Epstein
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Jay Wack
Thales UK Limited	Amit Sinha
Thales UK Limited	Devesh Tewari
Thales UK Limited	James Torjussen
The Clearing House	Mark Fitlin
The Clearing House	Sharon Jablon
The Clearing House	Hirak Patel
U.S. Bank	Stephen Case
University Bank	Stephen Ranzini
University Bank	Michael Talley
Utimaco Inc.	Susan Langford
Valley Bank	Mike Livni
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	Christophe Devaux
VeriFone, Inc.	Indra Fitzgerald
VeriFone, Inc.	Joachim Vance
Viewpointe	Richard Luchak
VISA	Adam Clark
VISA	Eric Le Saint
VISA	Kim Wagner
Wells Fargo Bank	Sotos Barkas
Wells Fargo Bank	Jason Buck
Wells Fargo Bank	David Cooper
Wells Fargo Bank	Goriola Dawodu
Wells Fargo Bank	Garrett Ellis
Wells Fargo Bank	Rameshchandra Ketharaju
Wells Fargo Bank	Antoinette McCarthy
Wells Fargo Bank	Kelly O'Donnell
Wells Fargo Bank	James Satterlee
Wells Fargo Bank	Jeff Stapleton
Wells Fargo Bank	Srinivas Voora
Whitebox Advisors	Heinrich Smit

© 2021 – All rights reserved

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

Stephen Case, Chairperson
Andrea Beatty, Vice Chairperson

Organization Represented	*Representative*
ACI Worldwide	Dan Kinney
ACI Worldwide	Julie Samson
Amazon	Sean Estrada
Amazon	Sandra Lambert
American Express Company	Gail Chapman
American Express Company	Alan Fong
American Express Company	Michael Hyzer
American Express Company	Peter Markall
American Express Company	Hing Too
American Express Company	Clyde Van Blarcum
American Express Company	Kevin Welsh
Bank of America	Amanda Adams
Bank of America	Dion Bellamy
Bank of America	Terrelle Carswell
Bank of America	Andi Coleman
Bank of America	Sean Fitzpatrick
Bank of America	Chuck Gruesbeck
Bank of America	Joel Kazin
Bank of America	Terry McKinney
Bank of America	Chris Schrick
Bank of America	Michael Shanzer
Bank of America	Matt Sharp
Bank of America	Michael Smith
Bank of America	Daniel Welch
Bank of America	Terri Willis
BBVA Compass	Stephanie DeCarlo
BBVA Compass	Omar Jarrar
BBVA Compass	Asia Pickle
BBVA Compass	Melinda Tobolewski
BetterBuyDesign	Steve Mott
Bloomberg LP	Erik Anderson
Capital One	Johnny Lee
comforte AG	Henning Horst
comforte AG	Michael Horst
Conexxus, Inc.	David Ezell
Conexxus, Inc.	Alan Thiemann
Conexxus, Inc.	Linda Toth
CUSIP Global Services	Scott Preiss
Delap LLP	Andrea Beatty
Delap LLP	Diane Bishop
Delap LLP	David Buchanan
Delap LLP	Spencer Giles
Diebold Nixdorf	Christoph Bruecher
Diebold Nixdorf	Rick Brunt
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Scott Harroff
Diebold Nixdorf	Anne Konecny
Diebold Nixdorf	Alexander Lindemeier
Diebold Nixdorf	Gennadij Liske
Diebold Nixdorf	Michael Nolte

© 2021 – All rights reserved

Diebold Nixdorf ..... David Phister
Diebold Nixdorf ..... Matthias Runowski
Digicert ..... Corey Bonnell
Digicert ..... Tim Hollebeek
Discover Financial Services ..... Debbie Holfeld
Discover Financial Services ..... Susan Pandy
Discover Financial Services ..... Julie Quandt
Discover Financial Services ..... Lakshmi Ramanathan
Discover Financial Services ..... Jordan Schaefer
Discover Financial Services ..... Jorge Vargas
Dover Fueling Solutions ..... Rohith Chinnaswamy
Dover Fueling Solutions ..... Henry Fieglein
Dover Fueling Solutions ..... Simon Siew
Dover Fueling Solutions ..... Harish Veeravalli
Federal Reserve Bank ..... Guy Berg
Federal Reserve Bank ..... Ken Han
Federal Reserve Bank ..... Ainsley Hargest
Federal Reserve Bank ..... Bob Hunt
Federal Reserve Bank ..... Paul Nunnally
Federal Reserve Bank ..... Patti Ritter
First National Bank of Omaha ..... Robert Lamagna-Reiter
First National Bank of Omaha ..... Sherry Rewolinski
First National Bank of Omaha ..... Kristi White
FIS ..... Tami Harris
FIS ..... Ian Lumsden
Fiserv ..... Bud Beattie
Fiserv ..... Scott Carpenter
Fiserv ..... Lisa Curry
Fiserv ..... Jacqueline Dill
Fiserv ..... Riquet Dominico
Fiserv ..... Angela Ghetu
Fiserv ..... Vinayak Kagalkar
Fiserv ..... Brian Kean
Fiserv ..... Michelle Matthews
Fiserv ..... Andres Mendoza
Fiserv ..... Dan Otten
Fiserv ..... Anthony Ringer
Fiserv ..... Bambi Tsui
Fiserv ..... Allisa Walker
Futurex ..... Comron Moeni
Futurex ..... Ryan Smith
Futurex ..... Tim Weston
GEOBRIDGE Corporation ..... Dean Macinskas
GEOBRIDGE Corporation ..... Jason Way
Gilbarco ..... Scott Spiker
Gilbarco ..... Scott Turner
Gilbarco ..... Bruce Welch
Hyosung TNS Inc. ..... Joe Militello
Hyosung TNS Inc. ..... JaeWhan Shin
Hyosung TNS Inc. ..... Nancy Walker
IBM Corporation ..... Wai Choi
IBM Corporation ..... Richard Kisley
ID TECH ..... Eric Lecesne
Ingenico ..... Steven Bowles
Ingenico ..... Vanessa Terrade
Ingram Micro ..... Candice Hoft
ISARA Corporation ..... Mike Brown

© 2021 – All rights reserved

ISARA Corporation	Philip Lafrance
ISARA Corporation	Alexander Truskovsky
ITS, Inc. (SHAZAM Networks)	Janet LaFrence
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Kathleen Krupa
J.P. Morgan Chase	Darryl Scott
K3DES LLC	James Richardson
MagTek, Inc.	Jeff Duncan
MagTek, Inc.	Mimi Hart
MasterCard Europe Sprl	Robert Gallagher
MasterCard Europe Sprl	Mark Kamers
MasterCard Europe Sprl	Michael Ward
Member Emeritus	Todd Arnold
Member Emeritus	Dave Faoro
Member Emeritus	Larry Hines
Member Emeritus	Darlene Kargel
Member Emeritus	Lawrence LaBella
Member Emeritus	Richard Sweeney
National Institute of Standards and Technology (NIST)	Elaine Barker
National Institute of Standards and Technology (NIST)	Lily Chen
National Institute of Standards and Technology (NIST)	Morris Dworkin
National Security Agency	Paul Timmel
NCR Corporation	Charlie Harrow
NCR Corporation	Bradford Loewy
NCR Corporation	Brian Wotherspoon
PAX Technology, Inc.	LeAnn Hostetler
PCI Security Standards Council	Leon Fell
PCI Security Standards Council	Troy Leach
PCI Security Standards Council	Doug Manchester
PCI Security Standards Council	John Markh
PCI Security Standards Council	Ralph Poore
PCI Security Standards Council	Randall Rieth
Publix Super Markets, Inc.	Jonathan Carter
Publix Super Markets, Inc.	Mark Clements
Publix Super Markets, Inc.	Joshua Peak
TECSEC Incorporated	Ed Scheidt
TECSEC Incorporated	Jay Wack
Thales UK Limited	Amit Sinha
Thales UK Limited	Devesh Tewari
Thales UK Limited	James Torjussen
The Clearing House	Sharon Jablon
The Clearing House	Jackie Pagán
U.S. Bank	Stephen Case
U.S. Bank	Dave Esmond
U.S. Bank	Victoria Evans
U.S. Bank	Stephanie Lane
University Bank	Stephen Ranzini
University Bank	Michael Talley
USDA Food and Nutrition Service	Erin McBride
Utimaco Inc.	Susan Langford
Utimaco Inc.	Manish Upasani
VeriFone, Inc.	John Barrowman
VeriFone, Inc.	Christophe Devaux
VeriFone, Inc.	Indra Fitzgerald
VeriFone, Inc.	Joachim Vance
VISA	Adam Clark

© 2021 – All rights reserved

VISA	Kim Wagner
Wells Fargo Bank	Troy Anderson
Wells Fargo Bank	Sotos Barkas
Wells Fargo Bank	Goriola Dawodu
Wells Fargo Bank	Garrett Ellis
Wells Fargo Bank	Matthew Greenwell
Wells Fargo Bank	Ryan Hegland
Wells Fargo Bank	Jeff Jacoby
Wells Fargo Bank	Rameshchandra Ketharaju
Wells Fargo Bank	Jan Kohl
Wells Fargo Bank	Eric Lengvenis
Wells Fargo Bank	Brian Parks
Wells Fargo Bank	Tim Plantand
Wells Fargo Bank	Abhijit Rao
Wells Fargo Bank	James Satterlee
Wells Fargo Bank	Jeff Stapleton
Wells Fargo Bank	Tony Stieber
Wells Fargo Bank	Richard Toohey
Wells Fargo Bank	Srinivas Voora
Wells Fargo Bank	David Walgamotte
Whitebox Advisors	Heinrich Smit

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

© 2021 – All rights reserved

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 card issuers.

© 2021 – All rights reserved

The scope of this part of X9.24 may apply to Internet-based transactions, but only when such applications include the use of a SCD (as defined in section 7.2 of ANS X9.24 Part 1) to protect the private and symmetric keys. This part of ANS X9.24 deals with management of symmetric keys using asymmetric techniques and storage of asymmetric private keys using symmetric keys. Additional parts may be created in the future to address other methods of key management.

This part of ANS X9.24 specifies the minimum requirements for the management of asymmetric keying material and symmetric keys used for ensuring the confidentiality and integrity of the private keys of asymmetric key pairs when stored as cryptograms on a database. Addressed are all components of the key management life cycle including generation, distribution, utilization, storage, archiving, replacement and destruction. Requirements for actions to be taken in the event of key compromise are also addressed. This part of ANS X9.24 presents overviews of the keys involved in the key transport and key agreement protocols, referencing other ANSI standards where applicable.

2.1 Application

This part of ANS X9.24 is applicable for institutions implementing techniques to ensure the confidentiality and integrity of asymmetric cryptographic key pairs used for the subsequent secure remote distribution of symmetric cryptographic keys.

Mandatory standard techniques and procedures are indicated by the word '**SHALL**'. Guidelines are indicated by the word '**SHOULD**'.

3 References

3.1 Normative References

The following publications SHALL be used in conjunction with this part of ANS X9.24. For dated references, only the specific edition cited applies. For undated references, the most recent edition of the referenced document (including any amendments) applies.

1. NIST SP800-67 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
2. ANS X9.24-1:2009 Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
3. ANS X9.102 Symmetric Key Cryptography For the Financial Services Industry – Wrapping of Keys and Associated Data
4. ISO 19592-2 Information technology- Security techniques - Secret sharing – Part 2: Fundamental mechanisms
5. ANS X9.8 Personal Identification Number (PIN) Management and Security
6. ANS X9.42 Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
7. ANS X9.44 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Factoring-Based Cryptography (draft)
8. ANS X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Management Using Elliptic Curve-Based Cryptography
9. ISO 21188 Public key infrastructure for financial services – Practices and Policy Framework

© 2021 – All rights reserved