X9 TR34–2012

Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport

A Technical Report prepared by:
Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Registered with American National Standards Institute

Date Registered: August 28, 2012

Contents

Page

Figures

Tables

Foreword

Publication of this Technical Report that has been registered with ANSI has been approved by the Accredited Standards Committee X9, Incorporated, 275 West Street, Suite 107, 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., 275 West Street, Suite 107, Annapolis, MD 21401,

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

The retail financial transactions industry needs a cost effective way to distribute the symmetric key materials required for financial cryptography. Physically visiting a remote terminal to enter keys is costly and error prone. An interoperable cryptographic protocol to distribute these keys using public cryptography techniques can provide a secure, cost effective solution. Manufacturers of both key distribution hosts and key receiving devices can then embed this protocol in the communication protocols used to interface hosts and devices. This Technical Report is intended to give the reader an implementation that meets the requirements for secure key distribution as set forth in ANS X9.24 Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys.

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, 275 West Street, Suite 107, Annapolis, MD 21401 USA.

This Technical Report was processed and registered for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the 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

Organization Represented	**Representative**	
ACI Worldwide	Doug	Grote
Advance Auto Parts	Anthony	Johnson
American Bankers Association	C. Diane	Poole
American Express Company	Vicky	Sammons
Apriva	Len	Sutton
BAFT/IFSA	Tod	Burwell
Bank of America	Daniel	Welch
BP Products North America	Robert	Slimmer
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Karla	McKenna
CUSIP Service Bureau	Gerard	Faulkner
Deluxe Corporation	Angela	Hendershott
Department of the Treasury, Office of Financial Research	Michael	Donnelly
Diebold, Inc.	Bruce	Chapa
Discover Financial Services	Michelle	Zhang
Federal Reserve Bank	Claudia	Swendseid
First Data Corporation	Rick	Van Luvender
FIS Global	Stephen	Gibson-Saxty
Fiserv	Dan	Otten

FIX Protocol Ltd - FPL	Jim	Northey
Gilbarco	Bruce	Welch
Harland Clarke	John	McCleary
Hewlett Packard	Larry	Hines
Independent Community Bankers of America	Viveca	Ware
Ingenico	John	Spence
ISITC	Genevy	Dimitrion
J.P. Morgan Chase	Roy	DeCicco
Key Innovations	Scott	Spiker
KPMG LLP	Mark	Lundin
MagTek, Inc.	Mimi	Hart
MasterCard Europe Sprl	Mark	Kamers
NACHA The Electronic Payments Association	Robert	Unger
National Association of Convenience Stores	Alan	Thiemann
National Security Agency	Paul	Timmel
NCR Corporation	Steve	Stevens
RouteOne	Travis	Bully
SWIFT/Pan Americas	Juliette	Kennel
Symcor Inc.	Brian	Salway
TECSEC Incorporated	Ed	Scheidt
The Clearing House	Sharon	Jablon
U.S. Securities and Exchange Commission	Paul	Knight
USDA Food and Nutrition Service	Kathy	Ottobre
Vantiv LLC	Patty	Walters
VeriFone, Inc.	Dave	Faoro
VISA	Kim	Wagner
Wells Fargo Bank	Mark	Tiggas
Wincor Nixdorf Inc	Ramesh	Arunashalam
XAC Automation Corporation	Chu	Nei
XBRL US, Inc.	Campbell	Pryde

The X9F subcommittee on Data & Information Security had the following members:

Ed Scheidt, X9F Chairman

Sandra Lambert, X9F Vice-Chairman

Organization Represented	**Representation**	
Acculynk	John	Herr
ACI Worldwide	Doug	Grote
Advance Auto Parts	Anthony	Johnson
American Bankers Association	Tom	Judd
American Express Company	Vicky	Sammons
Apriva	Paul	Coppinger
Bank of America	Andi	Coleman
BP Products North America	Robert	Slimmer
Burroughs Payments Systems, Inc.	David J.	Concannon
Certicom Corporation	Daniel	Brown
Citigroup, Inc.	Chii-Ren	Tsai
Communications Security Establishment	Jonathan	Hammell
Communications Security Establishment	Tara	Small
CUSIP Service Bureau	Scott	Preiss
DeLap LLP	Darlene	Kargel
Deluxe Corporation	Angela	Hendershott
Depository Trust and Clearing Corporation	Robert	Palatnick
Diebold, Inc.	Bruce	Chapa
Discover Financial Services	Jordan	Schaefer
Equinox Payments	Gary	Zempich
Federal Reserve Bank	Deb	Hjortland
First Data Corporation	Rick	Van Luvender
First National Bank of Omaha	Kristi	White
Fiserv	Bud	Beattie
GEOBRIDGE Corporation	Jason	Way
Gilbarco	Bruce	Welch
Harland Clarke	John	Petrie
Heartland Payment Systems	Scott	Meeker
Hewlett Packard	Larry	Hines
IBM Corporation	Todd	Arnold
Independent Community Bankers of America	Cary	Whaley
Ingenico	John	Spence
ITS, Inc. (SHAZAM Networks)	Manish	Nathwani
J.P. Morgan Chase	Glenn	Benson

K3DES LLC	Azie	Amini
Key Innovations	Scott	Spiker
KPMG LLP	Mark	Lundin
MagTek, Inc.	Mimi	Hart
Marriott International	Jude	Sylvestre
MasterCard Europe Sprl	Michael	Ward
Mustang Microsystems, Inc.	Tami	Harris
National Association of Convenience Stores	Alan	Thiemann
National Institute of Standards and Technology	Elaine	Barker
National Security Agency	Paul	Timmel
NCR Corporation	Charlie	Harrow
PCI Security Standards Council	Troy	Leach
Proofspace	Paul	Doyle
Rosetta Technologies	Jim	Maher
RSA, The Security Division of EMC	Steve	Schmalz
Security Innovation	Mark	Etzel
Security Innovation	William	Whyte
STAR	Lilik	Kazaryan
Surety, Inc.	Dimitrios	Andivahis
Symcor Inc.	Brian	Salway
TECSEC Incorporated	Ed	Scheidt
Thales e-Security, Inc.	James	Torjussen
The Clearing House	Henry	Farrar
Trustwave	John	Amaral
University Bank	Michael	Talley
Vantiv LLC	Patty	Walters
VeriFone, Inc.	Dave	Faoro
VISA	Kim	Wagner
Voltage Security, Inc.	Terence	Spies
Wells Fargo Bank	Jim	Hinsey
Wincor Nixdorf Inc	Ramesh	Arunashalam
XAC Automation Corporation	Chu	Nei

Under ASC X9, Inc. procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or technical report(s) in a specific area and is then disbanded. 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 technical report. (Note: Per X9 policy, company names of non-member participants are listed only if, at the time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F6 Cardholder Authentication and ICC's group which developed this technical report had the following members:

Scott Spiker, Chairman

Sid Sidner, Project Editor

Dan Kinney, Project Editor

Organization Represented	Representative	
Acculynk	John	Herr
Acculynk	Philip	Patrick
ACI Worldwide	Karl	Brown
ACI Worldwide	Charles	Collins
ACI Worldwide	Richard	DuVall
ACI Worldwide	Doug	Grote
ACI Worldwide	Dan	Kinney
ACI Worldwide	Julie	Samson
American Bankers Association	Tom	Judd
American Express Company	William J.	Gray
American Express Company	Vicky	Sammons
Apriva	Len	Sutton
Bank of America	Dion	Bellamy
Bank of America	Peter	Capraro
Bank of America	Terrelle	Carswell
Bank of America	Andi	Coleman
Bank of America	Chris	Schrick
Bank of America	Jeff	Stapleton
Bank of America	Daniel	Welch
BP Products North America	Robert	Slimmer
Burroughs Payments Systems, Inc.	David J.	Concannon
Burroughs Payments Systems, Inc.	Navnit	Shah
Certicom Corporation	Daniel	Brown
Certicom Corporation	Matt	Campagna
Certicom Corporation	John O.	Goyo
Certicom Corporation	Sandra	Lambert
Cirque Inc.	Keith	Paulsen
Citigroup, Inc.	Chii-Ren	Tsai
Clearkey, Inc.	Paul	Reimer
CUSIP Service Bureau	Scott	Preiss
CUSIP Service Bureau	James	Taylor
DeLap LLP	David	Buchanan
DeLap LLP	Stephen	Case
DeLap LLP	Darlene	Kargel
Depository Trust and Clearing Corporation	Robert	Palatnick
Diebold, Inc.	Rick	Brunt
Diebold, Inc.	Bruce	Chapa
Diebold, Inc.	Scott	Harroff

Diebold, Inc.	Anne	Konecny
Diebold, Inc.	Jessica	Walpole
Discover Financial Services	Mia	Boom-Ibes
Discover Financial Services	David	Kloser
Discover Financial Services	Jordan	Schaefer
Discover Financial Services	Michelle	Zhang
Dresser Wayne	Steven	Bowles
Dresser Wayne	Tom	Chittenden
Dresser Wayne	Tim	Weston
Equinox Payments	Mohammad	Arif
Equinox Payments	Alan	Fong
Equinox Payments	Gary	Zempich
Federal Reserve Bank	Jeremy	Brotherton
Federal Reserve Bank	Darin	Contini
Federal Reserve Bank	Pieralberto	Deganello
Federal Reserve Bank	Deb	Hjortland
Federal Reserve Bank	Mary	Hughes
Federal Reserve Bank	Kathleen	Jacob
Federal Reserve Bank	Joonho	Lee
Federal Reserve Bank	Mike	Ram
Ferris and Associates, Inc.	J. Martin	Ferris
Ferris and Associates, Inc.	Lynda R.	Strickland
First Data Corporation	Andrea	Beatty
First Data Corporation	Lisa	Curry
First Data Corporation	Lilik	Kazaryan
First Data Corporation	Brian	Kean
First National Bank of Omaha	Kristi	White
Fiserv	Bud	Beattie
Fiserv	Mary	Bland
Fiserv	Dennis	Freiburg
Fiserv	Dan	Otten
Futurex	Chris	Hamlett
Futurex	Jim	Lambert
Futurex	Ryan	Smith
GEOBRIDGE Corporation	Dean	Macinskas
GEOBRIDGE Corporation	Jason	Way
Gilbarco	Bruce	Welch
Harland Clarke	John	McCleary
Harland Clarke	John	Petrie
Heartland Payment Systems	Scott	Meeker
Hewlett Packard	Larry	Hines

Hewlett Packard	Susan	Langford
IBM Corporation	Todd	Arnold
IBM Corporation	Michael	Kelly
Independent Community Bankers of America	Cary	Whaley
Ingenico	Steve	McKibben
Ingenico	John	Spence
ITS, Inc. (SHAZAM Networks)	Manish	Nathwani
J.P. Morgan Chase	Bruce	Geller
J.P. Morgan Chase	Edward	Koslow
J.P. Morgan Chase	Kathleen	Krupa
J.P. Morgan Chase	Donna	Meagher Gem
J.P. Morgan Chase	Jackie	Pagan
J.P. Morgan Chase	Thomas	Pageler
K3DES LLC	Azie	Amini
K3DES LLC	James	Richardson
Key Innovations	Scott	Spiker
KPMG LLP	Mark	Lundin
MagTek, Inc.	Terry	Benson
MagTek, Inc.	Jeff	Duncan
MagTek, Inc.	Mimi	Hart
MagTek, Inc.	Larry	Meyers
Marriott International	Jude	Sylvestre
MasterCard Europe Sprl	Jeanne	Moore
MasterCard Europe Sprl	Susie	Thompson
MasterCard Europe Sprl	Michael	Ward
Mustang Microsystems, Inc.	Tami	Harris
National Association of Convenience Stores	Ann	Seki
National Association of Convenience Stores	Alan	Thiemann
National Institute of Standards and Technology	Elaine	Barker
National Institute of Standards and Technology	Lawrence	Bassham III
National Institute of Standards and Technology	William	Burr
National Institute of Standards and Technology	Lily	Chen
National Institute of Standards and Technology	David	Cooper
National Institute of Standards and Technology	Morris	Dworkin
National Institute of Standards and Technology	Randall	Easter
National Institute of Standards and Technology	Sharon	Keller
National Institute of Standards and Technology	Annabelle	Lee
National Institute of Standards and Technology	Fernando	Podio
National Security Agency	Paul	Timmel
NCR Corporation	Charlie	Harrow
NCR Corporation	Ali	Lowden

NCR Corporation	David	Norris
NCR Corporation	Ron	Rogers
NCR Corporation	Steve	Stevens
NCR Corporation	Ally	Whytock
PCI Security Standards Council	Leon	Fell
PCI Security Standards Council	Troy	Leach
PCI Security Standards Council	Ralph	Poore
Rosetta Technologies	Jim	Maher
RSA, The Security Division of EMC	Steve	Schmalz
SafeNet, Inc.	Chris	Dunn
SafeNet, Inc.	Terry	Fletcher
SafeNet, Inc.	Skip	Norton
SafeNet, Inc.	Kuldeep	Saini
SafeNet, Inc.	Brett	Thompson
Security Innovation	Mark	Etzel
Security Innovation	Jeff	Hoffstein
Security Innovation	William	Whyte
STAR	Lisa	Besack
STAR	Scott	Quinn
STAR	Robert	Ribble
Surety, Inc.	Dimitrios	Andivahis
Symcor Inc.	Brian	Salway
TECSEC Incorporated	Ed	Scheidt
TECSEC Incorporated	Dr. Wai	Tsang
TECSEC Incorporated	Jay	Wack
Thales e-Security, Inc.	Colette	Broadway
Thales e-Security, Inc.	Jose	Diaz
Thales e-Security, Inc.	Tim	Fox
Thales e-Security, Inc.	James	Torjussen
The Clearing House	Henry	Farrar
The Clearing House	Susan	Long
Trustwave	John	Amaral
Trustwave	Tim	Hollebeek
Trustwave	Patrick	McGregor
Trustwave	Alexander	Volynkin
University Bank	Stephen	Ranzini
University Bank	Michael	Talley
USDA Food and Nutrition Service	Kathy	Ottobre
Vantiv LLC	Dick	Bloss
Vantiv LLC	Tom	Humphrey
Vantiv LLC	Scott	Mackelprang

Vantiv LLC	Patty	Walters
Vantiv LLC	Bill	Weingart
Vantiv LLC	James	Zerfas
VeriFone, Inc.	John	Barrowman
VeriFone, Inc.	LeAnn	Brown
VeriFone, Inc.	David	Ezell
VeriFone, Inc.	Dave	Faoro
VeriFone, Inc.	Chris	Madden
VeriFone, Inc.	Doug	Manchester
VeriFone, Inc.	Brad	McGuinness
VeriFone, Inc.	Joachim	Vance
VISA	Amy	Brown
VISA	Leon	Fell
VISA	Hap	Huynh
VISA	Tara	Kissoon
VISA	Chackan	Lai
VISA	Stoddard	Lambertson
VISA	Chris	McDaniel
VISA	John	Sheets
VISA	Michael	Stefanich
VISA	Johan	Van Tilburg
VISA	Kim	Wagner
Voltage Security, Inc.	Luther	Martin
Voltage Security, Inc.	Terence	Spies
Voltage Security, Inc.	Richard	Sweeney
Wells Fargo Bank	William	Felts, IV
Wells Fargo Bank	Andrew	Garner
Wells Fargo Bank	Jeff	Jacoby
Wells Fargo Bank	Brian	Keltner
Wells Fargo Bank	Eric	Lengvenis
Wells Fargo Bank	David	Naelon
Wells Fargo Bank	Brian	Parks
Wells Fargo Bank	Doug	Pelton
Wells Fargo Bank	Chuck	Perry
Wells Fargo Bank	Marv	Peterson
Wells Fargo Bank	Keith	Ross
Wells Fargo Bank	Mike	Rudolph
Wells Fargo Bank	Mark	Tiggas
Wincor Nixdorf Inc	Christoph	Bruecher
Wincor Nixdorf Inc	Andrea	Carozzi
Wincor Nixdorf Inc	Michael	Nolte

Wincor Nixdorf Inc	Matthias	Runowski

This document is the first release of this technical report.

This document is used in conjunction with ANSI X9.24-2.

Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques: Part 1 – Using Factoring-Based Public Key Cryptography Unilateral Key Transport

1 Scope

This document describes a method consistent with the requirements of ANS X9.24-2 Retail Financial Services Symmetric Key Management - Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys for the secure exchange of keys using asymmetric techniques between two devices that share asymmetric keys. This method is designed to operate within the existing capabilities of devices used in the retail financial services industry.

This is an implementation of the Unilateral Key Transport Method defined in ANS X9.24-2.

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.

ANS X9.24-2 describes the security requirements for systems that distribute symmetric keys using asymmetric techniques. The security requirements are consistent across all systems; ANS X9.24-2 does not distinguish between types of systems or alter the security requirements depending upon the environment of the entities in the system. While this is the correct approach for security requirements, the implementation requirements on systems will vary depending upon the properties of the system.

This document specifies an interoperable method for one particular situation – the Distribution of Symmetric Keys using Asymmetric Techniques from a Single Key Distribution Host (KDH) to many Key Receiving Devices (KRDs). The KDH is assumed to be operated in a controlled environment (as specified in reference 4); the KRDs may operate in uncontrolled environments.

This interoperable method could also be used to exchange keys between peers, where one is administratively designated as the KDH and one as the KRD.

The KDH and the KRD are assumed to have an administrative understanding of the type and key characteristics of the symmetric key that is exchanged, as for a terminal master key. As such, the key exchanged is treated by this protocol as a binary blob.

This document uses the term KRD to denote the Key Receiving Device; The KRD is a Tamper Resistant Security Module (TRSM) such as a PIN Encrypting Device (PED), a Encrypting PIN PAD (EPP), or a Host Security Module (HSM).

Within the confines of this protocol, the KRD can only respond to commands from a KDH, i.e. the KRD is a slave KRD.