X9/TG-9–1995

Financial Services Technical Guideline
Developed By Accredited
Standards Committee
X9 – Financial Services

ABSTRACT SYNTAX NOTATION & ENCODING RULES FOR FINANCIAL INDUSTRY STANDARDS

Developed by
Accredited Standards Committee
X9 – Financial Services

Abstract Syntax Notation & Encoding Rules for Financial Industry Standards

This tutorial is for readers who wish to understand Abstract Syntax Notation One (ASN.1), the international standard language for defining and encoding data elements in the open systems environment. ASN.1 provides for a more precise specification of message fields and other data, improving interoperability and reducing costs. TG-9 familiarizes the reader with ASN.1 concepts in ISO/IEC 8824 Specification of ASN.1 and ISO/IEC 8825 Specification for Basic Encoding Rules for ASN.1.

Developed by the
Accredited Standards Committee
X9 – Financial Services
operating under the procedures of the
American National Standards Institute

Published by:

Accredited Standards Committee X9, Inc.
P.O. Box 4035
Annapolis, Maryland 21403 USA
Phone: 410-267-7707 or 301-879-7988
Fax: 301-879-5124
Email: Cindy.Fuller@X9.org
Isabel.Bailey@X9.org
X9 Online: http://www.x9.org

Printed in the United States of America

Contents

Figures

Tables

Blank page

Foreword

Several emerging X9 standards define data structures, such as certificates, using Abstract Syntax Notation One (ASN.1). ASN.1 is a language for specifying data types and values of those types. In this respect, it can be thought of as a programming language whose syntax allows the definition of complex data structures. Several sets of encoding rules, for representing instances of these data structures during communication between two entities, are also defined. For example, the Basic Encoding Rules (BER) encodes a data item as a set of three fields: identifier octets, length octets. and contents octets. Other sets of encoding rules are optimized for various network environments or other criteria.

This document presents an overview of those ASN.1 mechanisms used by the X9 standards. The references below cite the base standards and other useful documents dealing with ASN.1. It is suggested that protocol designers use ASN.1 to specify data types, and use the standard encoding rules to convey these data types in an open systems environment.

This is a tutorial document designed to familiarize the reader of other X9 standards with ASN.1 to a sufficient degree as to be able to understand the notation used in those standards, without requiring the reader to obtain and read the international standards covering ASN.1. In the event of contradictions between this guideline and the international standards, the latter are always to be used as the authoritative document.

Suggestions for the improvement or revision of this standard are welcome. They should be sent to Accredited Standards Committee X9, Inc., P.O. Box 4035, Annapolis, Maryland, 21403, USA.

This guideline was processed and approved by the Accredited Standards Committee X9 – Financial Services. Committee approval of this guideline does not necessarily imply that all committee members voted for its approval. At the time it approved this guideline, the X9 Committee had the following members:

Harold G. Deal, Chairman
Jack Kilhefner, Vice Chairman, Administration
Eileen Bell, Vice Chairman, Marketing
Cynthia L. Fuller, Associate Director, ABA Standards Division
Deborah Katz, Assistant Division Manager, ABA Standards Division

Organization Represented	*Name of Representative*
Advantis	Lori Eisenstaedt
American Bankers Association	Anne Livingston
American Express Company	Eileen Bell
Applied Communications	Barry Rhodes
AT&T Global Information Solutions	Robert K. Kramer
Bank of America	Gretchen Breiling
Canadian Bankers Association	Tom Anderson
Canadian Imperial Bank of Commerce	Dan Conlon
Chase Manhattan Bank, N.A.	John McKessey
Chemical Bank, N.A.	Francis J. Keenan
Citicorp	Seymour R. Rosen
Continental Bank, N.A.	Wayne E. Sochacki
CoreStates Bank	Kent Seinfeld
Deluxe Corporation	James Gallup
Discover Card Services, Inc.	Bill Kabat
Federal Reserve Bank	Michael Garrett
IBM Corporation	Harry Hankla
MasterCard International	Alice Droogan
Mellon Bank, N.A.	David P. Taddeo
Moore Business Forms, Inc.	Delmer Oddy
National Security Agency	Gerard A. Rainville, Jr.
NationsBanc Services, Inc.	Harold G. Deal
New York Clearing House Assn.	Vincent De Santis
Nat'l Institute of Science & Technology	Miles Smid
PNC Financial Corporation	John Ericksen
UNISYS Corporation	Karl T Sammons
VISA International	Patricia Greenhalgh
Wells Fargo Bank	Jack Kilhefner
XEROX Corporation	Mike Oszczakiewicz

The X9F Subcommittee on Data and Information Security had the following members:

J. Martin Ferris, Chairman

Organization Represented	*Name of Representative*
American Bankers Association	Gregg Broomfield
Applied Communications	David Phillips
Chase Manhattan Bank	Emil D'Angelo
Chemical Bank, N.A.	Joan Reynolds
Cylink	Sherry McMahan
Federal Reserve Bank	James Berlin
Fischer International	Richard Ankney
IBM Corporation	James Randall
Kirchman Corporation	Blair Rugh
Mellon Bank	Dain Gary
National Institute of Standards & Technology	Miles Smid
National Security Agency	Gerard Rainville
NationsBanc Services, Inc.	Don Sawyer
Northern Telecom	Beth Hardison
Racal-Guardata	Samuel Epstein
U.S. Department of Treasury	Martin Ferris
VISA International	Bill Chen

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

Working Group X9F1, which reported to X9F and which developed this guideline, included the following participants:

M. Blake Greenlee, Chairman

Chemical Bank	Peggy Bruner
Chemical Bank	Joan Murray Reynolds
Citibank	Sandra M. Lambert
Fischer International	Richard Ankney
IBM	Don B. Johnson
IBM	James Randall
MasterCard International	Jeff J. Stapleton
Mobius Encryption Technologies	Sherry Shannon
Natl Inst of Stds & Technology	Elaine Barker
Natl Inst of Stds & Technology	Miles Smid
National Security Agency	Gerard Rainville
National Security Agency	Clarence Reaver
Northern Telecom	Warwick Ford
VISA International	Bill Chen

Other participants

Donald Holden
Julie Smith McEwen
Paul Van Oorshot
Frank Sudia

Blank page

Abstract Syntax Notation & Encoding Rules for Financial Industry Standards

1 Introduction

Several emerging ANSI X9 standards define data structures, such as certificates, using Abstract Syntax Notation One (ASN.1). ASN.1 is a language for specifying data types and values of those types. In this respect, it can be thought of as a programming language whose syntax allows the definition of complex data structures. Several sets of encoding rules, for representing instances of these data structures during communication between two entities, are also defined. For example, the Basic Encoding Rules (BER) encodes a data item as a set of three fields: identifier octets, length octets. and contents octets. Other sets of encoding rules are optimized for various network environments or other criteria.

1.1 Scope and organization

This document presents an overview of those ASN.1 mechanisms used by the X9 standards. The references below cite the base standards and other useful documents dealing with ASN.1. It is suggested that protocol designers use ASN.1 to specify data types, and use the standard encoding rules to convey these data types in an open systems environment. This document suggests several other encoding mechanisms for use in 7-bi ASCII and other environments which do not support transparent 8-bit communication. Regardless of the communications environment (and encoding scheme), the emphasis of the document is on using ASN.1 as a specification tool.

Section 2 of this document defines the syntax used to specify ASN.1 types. Section 3 defines some extensions to the basic type notation. Section 4 presents one set of encoding rules (the Basis Encoding Rules (BER)), and discusses some other encoding rules. Section 5 presents some examples, and Section 6 lists references used in the preparation of the guideline.

The intent of this document is to describe the use of ASN.1 as a specification tool, to a sufficient level of detail to understand the types defined in the X9 security standards. Information on representation schemes is presented to illustrate the requirements on encoding schemes which might be developed by X9, and to aid the reader in evaluating conformance of ASN.1 compilers and other products to the base standards (see references 2-6). This document is **not** meant to be the sole source used to implement such ASN.1 tools, however. Implementors should obtain the base standards, as this document does not present all features of ASN.1 to a sufficient level of detail for implementation.

1.2 History

X.409 was developed by CCITT in 1984 for use in the X.400 Message Handling System (MHS). Other Open Systems Interconnect (OSI) application protocol designers quickly recognized that the language defined in X.409 had much wider application than just

MHS, so X.409 was restructured into X.208 (ISO/IEC 8824) and X.209 (ISO/IEC 8825) and moved to the X.200 series of Recommendations in 1988, and a number of useful features were added.

In 1992, several alternative sets of encoding rules were defined, the type notation was extended to allow parameterized types, and the macro notation defined in X.208 was replaced with tools for defining classes of information objects.

Most OSI application protocols now use ASN.1 for both data structure definition (abstract syntax, in OSI terminology) and encoding for transmission (transfer syntax); these include:

- Network Management (X.700),
- Directories (X.500),
- Message Handling (X.400), and
- File Transfer.

1.3 Terminology

A type is a named set of values (possibly unlimited in size). The structure of a value is determined by its type specification. ASN.1 defines a number of primitive types, e.g., integers and bit strings. New data types are defined by combining a small number of these primitive types in various ways