

American National Standard

INCITS/ISO/IEC 8825-1:2015 (2019)

(ISO/IEC 8825-1:2015, IDT)

Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

Developed by



Where IT all begins



INCITS/ISO/IEC 8825-1:2015 (2019)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.

Date of ANSI Approval: 11/22/2019

Published by American National Standards Institute,
25 West 43rd Street, New York, New York 10036

Copyright 2019 by Information Technology Industry Council
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

Fifth edition
2015-11-15

Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

*Technologies de l'information — Règles de codage ASN.1:
Spécification des règles de codage de base (BER), des règles de
codage canoniques (CER) et des règles de codage distinctives (DER)*

Reference number
ISO/IEC 8825-1:2015(E)



This is a preview of "INCITS/ISO/IEC 8825-...". Click here to purchase the full version from the ANSI store.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

This is a preview of "INCITS/ISO/IEC 8825-...". [Click here to purchase the full version from the ANSI store.](#)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

This fifth edition cancels and replaces the fourth edition of ISO/IEC 8825-1:2008 which has been technically revised. It also incorporates ISO/IEC 8825-1:2008/Cor.1:2012 and ISO/IEC 8825-5:2008/Cor.2:2014.

ISO/IEC 8825-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T X.690 (08/2015).

This is a preview of "INCITS/ISO/IEC 825-...". [Click here to purchase the full version from the ANSI store.](#)

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.690

(08/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

OSI networking and system aspects – Abstract Syntax
Notation One (ASN.1)

**Information technology – ASN.1 encoding rules:
Specification of Basic Encoding Rules (BER),
Canonical Encoding Rules (CER) and
Distinguished Encoding Rules (DER)**

Recommendation ITU-T X.690

PUBLIC DATA NETWORKS	
Services and facilities	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalling and switching	X.50–X.89
Network aspects	X.90–X.149
Maintenance	X.150–X.179
Administrative arrangements	X.180–X.199
OPEN SYSTEMS INTERCONNECTION	
Model and notation	X.200–X.209
Service definitions	X.210–X.219
Connection-mode protocol specifications	X.220–X.229
Connectionless-mode protocol specifications	X.230–X.239
PICS proformas	X.240–X.259
Protocol Identification	X.260–X.269
Security Protocols	X.270–X.279
Layer Managed Objects	X.280–X.289
Conformance testing	X.290–X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300–X.349
Satellite data transmission systems	X.350–X.369
IP-based networks	X.370–X.379
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600–X.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
Systems management framework and architecture	X.700–X.709
Management communication service and protocol	X.710–X.719
Structure of management information	X.720–X.729
Management functions and ODMA functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	
Commitment, concurrency and recovery	X.850–X.859
Transaction processing	X.860–X.879
Remote operations	X.880–X.889
Generic applications of ASN.1	X.890–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	X.1000–X.1099
SECURE APPLICATIONS AND SERVICES	X.1100–X.1199
CYBERSPACE SECURITY	X.1200–X.1299
SECURE APPLICATIONS AND SERVICES	X.1300–X.1399
CYBERSECURITY INFORMATION EXCHANGE	X.1500–X.1599
CLOUD COMPUTING SECURITY	X.1600–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

Summary

Recommendation ITU-T X.690 | ISO/IEC 8825-1 defines a set of Basic Encoding Rules (BER) that may be applied to values of types defined using the ASN.1 notation. Application of these encoding rules produces a transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also used for decoding. This Recommendation | International Standard defines also a set of Distinguished Encoding Rules (DER) and a set of Canonical Encoding Rules (CER) both of which provide constraints on the Basic Encoding Rules (BER). The key difference between them is that DER uses the definite length form of encoding while CER uses the indefinite length form. DER is more suitable for the small encoded values, while CER is more suitable for the large ones. It is implicit in the specification of these encoding rules that they are also used for decoding.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.690	1994-07-01	7	11.1002/1000/3046
1.1	ITU-T X.690 (1994) Technical Cor. 1	1995-11-21	7	11.1002/1000/3283
1.2	ITU-T X.690 (1994) Technical Cor. 2	1997-12-12	7	11.1002/1000/4182
1.3	ITU-T X.690 (1994) Technical Cor. 3	1997-12-12	7	11.1002/1000/4183
2.0	ITU-T X.690	1997-12-12	7	11.1002/1000/4447
2.1	ITU-T X.690 (1997) Technical Cor. 1	1999-06-18	7	11.1002/1000/4705
2.2	ITU-T X.690 (1997) Amd. 1	1999-06-18	7	11.1002/1000/4704
2.3	ITU-T X.690 (1997) Technical Cor. 2	2001-02-02	7	11.1002/1000/5335
3.0	ITU-T X.690	2002-07-14	17	11.1002/1000/6089
3.1	ITU-T X.690 (2002) Amd. 1	2003-10-29	17	11.1002/1000/7021
3.2	ITU-T X.690 (2002) Amd. 2	2006-06-13	17	11.1002/1000/8838
3.3	ITU-T X.690 (2002) Technical Cor. 1	2007-05-29	17	11.1002/1000/9108
4.0	ITU-T X.690	2008-11-13	17	11.1002/1000/9608
4.1	ITU-T X.690 (2008) Cor. 1	2011-10-14	17	11.1002/1000/11378
4.2	ITU-T X.690 (2008) Cor. 2	2014-03-01	17	11.1002/1000/12147
5.0	ITU-T X.690	2015-08-13	17	11.1002/1000/12483

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2015

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	<i>Page</i>
Introduction	v
1 Scope	1
2 Normative references.....	1
2.1 Identical Recommendations International Standards	1
2.2 Additional references	1
3 Definitions	1
4 Abbreviations	2
5 Notation	2
6 Convention	2
7 Conformance	3
8 Basic encoding rules.....	3
8.1 General rules for encoding	3
8.2 Encoding of a boolean value	6
8.3 Encoding of an integer value.....	6
8.4 Encoding of an enumerated value	7
8.5 Encoding of a real value.....	7
8.6 Encoding of a bitstring value.....	8
8.7 Encoding of an octetstring value	9
8.8 Encoding of a null value.....	10
8.9 Encoding of a sequence value	10
8.10 Encoding of a sequence-of value.....	10
8.11 Encoding of a set value	10
8.12 Encoding of a set-of value.....	11
8.13 Encoding of a choice value	11
8.14 Encoding of a value of a prefixed type.....	11
8.15 Encoding of an open type.....	12
8.16 Encoding of an instance-of value	12
8.17 Encoding of a value of the embedded-pdv type	12
8.18 Encoding of a value of the external type.....	12
8.19 Encoding of an object identifier value.....	13
8.20 Encoding of a relative object identifier value.....	14
8.21 Encoding of an OID internationalized resource identifier value	14
8.22 Encoding of a relative OID internationalized resource identifier value	15
8.23 Encoding for values of the restricted character string types.....	15
8.24 Encoding for values of the unrestricted character string type	17
8.25 Encoding for values of the useful types	17
8.26 Encoding for values of the TIME type and the useful time types.....	17
9 Canonical encoding rules	17
9.1 Length forms	18
9.2 String encoding forms	18
9.3 Set components	18
10 Distinguished encoding rules.....	18
10.1 Length forms	18
10.2 String encoding forms	18
10.3 Set components	19
11 Restrictions on BER employed by both CER and DER	19
11.1 Boolean values	19
11.2 Unused bits.....	19
11.3 Real values	19

11.6	Set-of components.....	20
11.7	GeneralizedTime	20
11.8	UTCTime	20
11.9	The TIME type and the useful time types.....	21
12	Use of BER, CER and DER in transfer syntax definition	21
Annex A	– Example of encodings	23
A.1	ASN.1 description of the record structure	23
A.2	ASN.1 description of a record value	23
A.3	Representation of this record value	23
Annex B	– Identification of Encoding Rules	25
Annex C	– Illustration of real value encoding	26

Introduction

Rec. ITU-T X.680 | ISO/IEC 8824-1, Rec. ITU-T X.681 | ISO/IEC 8824-2, Rec. ITU-T X.682 | ISO/IEC 8824-3, Rec. ITU-T X.683 | ISO/IEC 8824-4 (Abstract Syntax Notation One or ASN.1) together specify a notation for the definition of abstract syntaxes, enabling application standards to define the types of information they need to transfer. It also specifies a notation for the specification of values of a defined type.

This Recommendation | International Standard defines encoding rules that may be applied to values of types defined using the ASN.1 notation. Application of these encoding rules produces a transfer syntax for such values. It is implicit in the specification of these encoding rules that they are also to be used for decoding.

There may be more than one set of encoding rules that can be applied to values of types that are defined using the ASN.1 notation. This Recommendation | International Standard defines three sets of encoding rules, called *basic encoding rules*, *canonical encoding rules* and *distinguished encoding rules*. Whereas the basic encoding rules give the sender of an encoding various choices as to how data values may be encoded, the canonical and distinguished encoding rules select just one encoding from those allowed by the basic encoding rules, eliminating all of the sender's options. The canonical and distinguished encoding rules differ from each other in the set of restrictions that they place on the basic encoding rules.

The distinguished encoding rules is more suitable than the canonical encoding rules if the encoded value is small enough to fit into the available memory and there is a need to rapidly skip over some nested values. The canonical encoding rules is more suitable than the distinguished encoding rules if there is a need to encode values that are so large that they cannot readily fit into the available memory or it is necessary to encode and transmit a part of a value before the entire value is available. The basic encoding rules is more suitable than the canonical or distinguished encoding rules if the encoding contains a set value or set-of value and there is no need for the restrictions that the canonical and distinguished encoding rules impose. This is due to the memory and CPU overhead that the latter encoding rules exact in order to guarantee that set values and set-of values have just one possible encoding.

Annex A gives an example of the application of the basic encoding rules. It does not form an integral part of this Recommendation | International Standard.

Annex B summarizes the assignment of object identifier and OID internationalized resource identifier values made in this Recommendation | International Standard. It does not form an integral part of this Recommendation | International Standard.

Annex C gives examples of applying the basic encoding rules for encoding reals. It does not form an integral part of this Recommendation | International Standard.

This is a preview of "INCITS/ISO/IEC 825-...". [Click here to purchase the full version from the ANSI store.](#)

This is a preview of "INCITS/ISO/IEC 8825-...". Click here to purchase the full version from the ANSI store.

Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

1 Scope

This Recommendation | International Standard specifies a set of basic encoding rules that may be used to derive the specification of a transfer syntax for values of types defined using the notation specified in Rec. ITU-T X.680 | ISO/IEC 8824-1, Rec. ITU-T X.681 | ISO/IEC 8824-2, Rec. ITU-T X.682 | ISO/IEC 8824-3, and Rec. ITU-T X.683 | ISO/IEC 8824-4, collectively referred to as Abstract Syntax Notation One or ASN.1. These basic encoding rules are also to be applied for decoding such a transfer syntax in order to identify the data values being transferred. It also specifies a set of canonical and distinguished encoding rules that restrict the encoding of values to just one of the alternatives provided by the basic encoding rules.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

NOTE – This Recommendation | International Standard is based on ISO/IEC 10646:2003. It cannot be applied using later versions of this standard.

2.1 Identical Recommendations | International Standards

- Recommendation ITU-T X.680 (2015) | ISO/IEC 8824-1:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*
- Recommendation ITU-T X.681 (2015) | ISO/IEC 8824-2:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*
- Recommendation ITU-T X.682 (2015) | ISO/IEC 8824-3:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*
- Recommendation ITU-T X.683 (2015) | ISO/IEC 8824-4:2015, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

2.2 Additional references

- ISO *International Register of Coded Character Sets to be used with Escape Sequences.*
- ISO/IEC 2022:1994, *Information technology – Character code structure and extension techniques.*
- ISO/IEC 2375:2003, *Information technology – Procedure for registration of escape sequences and coded character sets.*
- ISO 6093:1985, *Information processing – Representation of numerical values in character strings for information interchange.*
- ISO/IEC 6429:1992, *Information technology – Control functions for coded character sets.*
- ISO/IEC 10646:2003, *Information technology – Universal Multiple-Octet Coded Character Set (UCS).*

3 Definitions

For the purposes of this Recommendation | International Standard, the definitions of Rec. ITU-T X.200 | ISO/IEC 7498-1 and Rec. ITU-T X.680 | ISO/IEC 8824-1 and the following definitions apply.