

This is a preview of "INCITS/ISO/IEC 20060...". Click here to purchase the full version from the ANSI store.

INCITS/ISO/IEC 20060:2001[2008]  
(ISO/IEC 20060:2001, IDT)

# American National Standard

*Information technology —  
Open Terminal Architecture (OTA)  
specification — Virtual machine  
specification*

**Developed by**



*Where IT all begins*



This is a preview of "INCITS/ISO/IEC 20060...". [Click here to purchase the full version from the ANSI store.](#)

**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: 7/1/2008

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

Copyright 2008 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, 1250 Eye Street NW, Washington, DC 20005.  
Printed in the United States of America

This is a preview of "INCITS/ISO/IEC 20060...". [Click here to purchase the full version from the ANSI store.](#)

# Table of Contents

---

Foreword.....	ix
Introduction.....	x
Purpose.....	x
Subject.....	x
Audience.....	x
How This Standard is Organised .....	xi
Aids in Using This Standard.....	xi
Related Publications .....	xi
References .....	xii
<b>1 Scope</b>	<b>1 –1</b>
<b>2 Conventions</b>	<b>2–3</b>
2.1 Abbreviations.....	2–3
2.2 Glossary .....	2–4
2.3 Data Types .....	2–7
2.4 Stack Notation.....	2–8
2.5 Flags.....	2–8
<b>3 OTA Virtual Machine</b>	<b>3–9</b>
3.1 Introduction.....	3–9
3.2 Virtual Machine CPU.....	3–10
3.2.1 Registers .....	3–10
3.2.2 Virtual Machine Size and Cells .....	3–11
3.2.3 Memory.....	3–11
3.2.4 Stacks.....	3–11
3.2.5 Frame Mechanism and Usage.....	3–12
3.2.6 Extensible Memory .....	3–14
3.2.7 User Variables .....	3–14
3.3 Virtual Machine Execution Features.....	3–15
3.4 Arithmetic .....	3–15

This is a preview of "INCITS/ISO/IEC 20060...". Click here to purchase the full version from the ANSI store.

3.6 Resources .....	3-17
3.7 Programs and Tokens.....	3-18
<b>4 System Services</b>	<b>4-19</b>
4.1 Time Handling .....	4-19
4.2 Devices and I/O Services.....	4-20
4.3 Database Services .....	4-21
4.3.1 The Database Parameter Block .....	4-22
4.3.2 Database Instantiation .....	4-24
4.3.3 Database Exception Handling .....	4-25
4.4 Language and Message Handling.....	4-25
4.5 TLV Services .....	4-26
4.5.1 Basic Principles .....	4-26
4.5.2 TLV Definitions .....	4-27
4.5.3 TLV References.....	4-28
4.6 Hot Card List Management .....	4-28
4.7 Cryptographic Services.....	4-29
4.7.1 Modulo Multiplication .....	4-30
4.7.2 Secure Hash Algorithm (SHA-1) .....	4-30
4.7.3 Modulo Exponentiation.....	4-30
4.7.4 Long Shift .....	4-30
4.7.5 Long Subtract .....	4-31
4.7.6 Incremental Secure Hash Algorithm (SHA-1).....	4-31
4.7.7 Cyclic Redundancy Check (CRC) .....	4-31
4.7.8 DES Key Schedule.....	4-32
4.7.9 DES encryption/decryption .....	4-32
4.8 Vectored Execution Sockets .....	4-32
4.8.1 CSS Functions .....	4-33
4.8.2 Socket Security .....	4-33
4.8.3 Socket Organisation .....	4-33
4.9 Module Handling Services .....	4-33
4.9.1 Module Loading by <b>MODEXECUTE</b> .....	4-34
4.9.2 Module Loading Procedure.....	4-37
4.9.3 Module Loading by <b>MODCARDEXECUTE</b> .....	4-39
<b>5 Token Set Definition</b>	<b>5-43</b>
5.1 Overview.....	5-43
5.2 Conventions .....	5-43
5.2.1 Number Formats .....	5-43
5.2.2 Token Descriptions .....	5-43
5.2.3 Branch and Code Offsets .....	5-44
5.2.4 Addresses.....	5-44
5.3 Data Typing .....	5-44

This is a preview of "INCITS/ISO/IEC 20060...". [Click here to purchase the full version from the ANSI store.](#)

5.4.1 Optimised Data Access.....	5-45
5.4.2 Special Procedure Calls .....	5-45
5.4.3 Quoting.....	5-45
5.5 Prefix Tokens .....	5-46
5.6 Stack Manipulation Tokens.....	5-47
5.7 Data Access Tokens .....	5-49
5.8 Literal Tokens .....	5-51
5.9 Address Generation Tokens .....	5-52
5.10 Arithmetic Tokens.....	5-53
5.11 Relational Tokens.....	5-55
5.12 String Tokens .....	5-57
5.13 Frame Tokens.....	5-60
5.14 Extensible Memory Tokens .....	5-62
5.15 Flow of Control Tokens .....	5-63
5.15.1 Branch Tokens .....	5-63
5.15.2 Call Tokens .....	5-64
5.15.3 Loop Tokens.....	5-65
5.15.4 Hybrid Tokens.....	5-66
5.15.5 Quoting Tokens .....	5-66
5.16 Exception Tokens.....	5-67
5.17 Date, Time, and Timing Tokens.....	5-67
5.18 Generic Device I/O Tokens.....	5-68
5.19 Formatted I/O Tokens .....	5-71
5.20 Integrated Circuit Card Tokens .....	5-72
5.21 Magnetic Stripe Tokens .....	5-73
5.22 Socket Tokens .....	5-75
5.23 Database Services Tokens.....	5-76
5.24 Language and Message Tokens .....	5-80
5.25 TLV Tokens.....	5-81
5.25.1 TLV Buffer Access .....	5-82
5.25.2 TLV Processing.....	5-83
5.25.3 TLV Sequence Access .....	5-85
5.26 Hot Card List Tokens .....	5-85
5.27 Cryptographic Algorithm Token.....	5-86
5.28 Module Management Tokens.....	5-86
5.29 Operating System Interface Tokens .....	5-88
5.30 Miscellaneous Tokens .....	5-88

## **6 Module Delivery Format 6-91**

6.1 Module ID Format .....	6-92
6.2 Socket List .....	6-92

This is a preview of "INCITS/ISO/IEC 20060...". Click here to purchase the full version from the ANSI store.

6.4 Module Import List.....	6-94
6.5 Module Export List.....	6-94
6.6 Module Procedure List .....	6-94

**Appendix A: OTA Token Lists** **A-97**

A.1 Numeric List of Tokens .....	A-97
A.2 Alphabetic List of Tokens.....	A-100

**Appendix B: Exceptions and I/O Return Codes** **B-103**

B.1 Exceptions and IOR codes .....	B-103
------------------------------------	-------

**Appendix C: Device Control** **C-107**

C.1 Device References and Return Codes .....	C-107
C.2 Debug Device.....	C-109
C.3 Keyboard Handling .....	C-110
C.4 Display and Printer Output .....	C-111
C.5 Serial Port Management.....	C-115
C.6 Modem Handling .....	C-116
C.7 ICC Card Handling .....	C-117
C.8 Magnetic Stripe Handling .....	C-119
C.9 Power Management.....	C-120
C.10 Vending Machine Control.....	C-121

**Appendix D: Operating System Calls** **D-123**

**Appendix E: Rules for Using a Data Object List (DOL)** **E-125**

**Appendix F: System Overview** **F-127**

How This Appendix is Organised.....	F-127
F.1 Introduction .....	F-128
F.2 System Components .....	F-131
F.3 OTA System Features.....	F-135
F.4 Program Security and Integrity .....	F-142
F.5 OTA Software Development Tools.....	F-145
F.6 Summary of the Open Terminal Architecture .....	F-151

This is a preview of "INCITS/ISO/IEC 20060...". Click here to purchase the full version from the ANSI store.

## List of Figures

1. Virtual Machine architecture. . . . .	3-10
2. Frame management example. . . . .	3-13
3. Database memory access. . . . .	4-22
4. Module execution procedure. . . . .	4-36
5. Module loading procedure . . . . .	4-38
6. ICC module execution procedure . . . . .	4-40
7. OTA development environment . . . . .	F-131
8. Tokens in the OTA concept. . . . .	F-135
9. The OTA Virtual Machine. . . . .	F-136
10. Kernel development tools . . . . .	F-146
11. Application development tools . . . . .	F-147

## List of Tables

1. Data type designations used in OTA. . . . .	2-7
2. Virtual Machine registers . . . . .	3-10
3. Data that the VM may hold on the return stack . . . . .	3-12
4. User variables in the Virtual Machine. . . . .	3-14
5. Initial condition of the VM on entry to the TRS. . . . .	3-15
6. Optional general exceptions from ANS Forth. . . . .	3-17
7. Virtual Machine resources. . . . .	3-17
8. DPB Structure . . . . .	4-22
9. Messages, by number and orig in . . . . .	4-25
10. Message table format . . . . .	4-26
11. Cryptographic algorithm codes . . . . .	4-29
12. Result codes from <b>COMPARE</b> . . . . .	5-58
13. ISO parameter track selection codes. . . . .	5-74
14. Module delivery format. . . . .	6-91
15. Socket list in Module Delivery Format. . . . .	6-92
16. Relocation specification . . . . .	6-93
17. Module import list format. . . . .	6-94
18. Module export list format . . . . .	6-94
19. Module procedure list format . . . . .	6-95
20. ANS Forth <b>THROW</b> codes in OTA kernels. . . . .	B-103
21. OTA <b>THROW</b> codes . . . . .	B-104
22. OTA I/O return codes . . . . .	B-105
23. Device code assignments . . . . .	C-108
24. Token — device number cross reference . . . . .	C-109
25. Debug device I/O return codes . . . . .	C-109
26. Standard key mappings. . . . .	C-110
27. DEVIOCTL parameters for keyboard device . . . . .	C-111
28. Keyboard device I/O return codes. . . . .	C-111
30. DEVIOCTL parameters for display device. . . . .	C-112
29. Control Code Interpretation . . . . .	C-112
31. DEVIOCTL parameters for printer device . . . . .	C-113
33. Printer device I/O return codes . . . . .	C-114
32. Display device I/O return codes . . . . .	C-114
34. DEVIOCTL parameters for serial port device . . . . .	C-115
35. Serial port device I/O return codes. . . . .	C-115
36. DEVIOCTL parameters for modem device . . . . .	C-116
37. Modem device I/O return codes . . . . .	C-117

This is a preview of "INCITS/ISO/IEC 20060...". [Click here to purchase the full version from the ANSI store.](#)

39. ICC card reader device I/O return codes . . . . .	C-118
40. DEVIOCTL parameters for magnetic card reader device. . . . .	C-119
41. Magnetic card reader I/O return codes . . . . .	C-119
42. DEVIOCTL parameters for power management device. . . . .	C-120
43. Power management device I/O return codes. . . . .	C-120
44. DEVIOCTL parameters for vending machine device. . . . .	C-121
45. Vending machine device I/O return codes. . . . .	C-121
46. OSCALL functions . . . . .	D-123
47. Virtual Machine registers . . . . .	F-136



This is a preview of "INCITS/ISO/IEC 20060...". [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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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 International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 20060 was prepared by Europay International and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

# Introduction

## Purpose

The Europay Open Terminal Architecture (OTA) consists of technology designed to facilitate implementation of Integrated Circuit Cards (ICCs) and associated terminals.

The purpose of this document is to provide a specification for a standard kernel to be provided in all OTA terminals.

## Subject

OTA defines a standard software kernel whose functions and programming interface are common across all terminal types. This kernel is based on a standard "Virtual Machine," which is implemented on each CPU type and which provides drivers for the terminal's I/O and all low-level CPU-specific logical and arithmetic functions. High-level libraries, terminal programs and payment applications may be developed using these standard kernel functions.

Additional volumes in this series describe Forth and C language bindings and compiler requirements.

## Audience

This document is intended for anyone desiring to evaluate OTA technology, develop OTA kernels, or develop payment programs or libraries designed to run on OTA kernels. General knowledge of computers and programming is assumed.

This is a preview of "INCITS/ISO/IEC 20060...". Click here to purchase the full version from the ANSI store.

This document is divided into the following chapters:

- Chapter 1 Management Summary* provides a summary of the key points that are developed in this book.
- Chapter 2 Conventions* describes notational and syntactic conventions used in this specification, as well as OTA data types supported and other general technical issues applying to subsequent chapters.
- Chapter 3 OTA Virtual Machine* describes the “Virtual Machine” architecture upon which OTA is based.
- Chapter 4 System Services* describes the various services provided by an OTA kernel to client programs.
- Chapter 5 Token Set Definition* provides a detailed specification of the OTA token set (the machine language of the “Virtual Machine”).
- Chapter 6 Module Delivery Format* describes the delivery package for tokenised external modules provided to OTA kernels.

## Aids in Using This Standard

This document contains the following aids for using the information it presents:

- A list of all of the tables present in this standard, found on page vi.
- A list of abbreviations referred to in this standard, found on page 2–3.
- A glossary of terms used in this standard, found on page 2–4.
- Numeric and alphabetic lists of OTA tokens, with page numbers, in Appendix A.
- A summary of exception codes and I/O result codes in Appendix B.
- A summary of current devices supported, with device numbers and control codes, in Appendix C.
- A list of operating system functions in Appendix D.
- Rules for TLV ‘Data Object List’ handling in Appendix E.
- Open Terminal Architecture System Overview in Appendix F.
- An index of topics covered in this standard, found at the end of the document.

## Related Publications

The following publications contain material directly related to the content of this standard. Available from original PAS submitter (see above).

- EMV2000, *Integrated Circuit Card Specification for Payment Systems, Book 1 - Applications Independent ICC to Terminal Interface Requirements*. Version 4.0, December 2000.<sup>1</sup>
- EMV2000, *Integrated Circuit Card Specification for Payment Systems, Book 2 - Security*

---

1. The EMV2000 documents may be obtained free of charge from EMVCo at <http://www.emvco.com>.

This is a preview of "INCITS/ISO/IEC 20060...". Click here to purchase the full version from the ANSI store.

- EMV2000, *Integrated Circuit Card Specification for Payment Systems, Book 3 - Application Specification*. Version 4.0, December 2000.
- EMV2000, *Integrated Circuit Card Specification for Payment Systems, Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements*. Version 4.0, December 2000.
- *Open Terminal Architecture (OTA) Specification Volume 2: Forth Language Programming Interface*. Version 3.0 Draft 2, July 3, 1998.
- *Open Terminal Architecture (OTA) Specification, Volume 3: C Language Programming Interface*. Version 1.3 – July 17, 1997.
- *Open Terminal Architecture (OTA) Specification, Volume 4: Mixed Language Programming*. Version 1.1 – July 1, 1997.
- *OTA Terminal Kernel Test Program (TKTP) Reference Manual. Version 4.5, Oct. 12, 1999.*

## References

The following references may be of use to the reader of this document:

ANSI X9.30-2:1997	Public key cryptography using irreversible algorithms for the financial services industry — Part 2: The Secure Hash Algorithm (SHA)
ANSI X9.31-1998	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
FIPS PUB 180-1:1994	Secure Hash Standard
ISO 639:1988	Codes for the representation of names and languages
ISO 3166-1:1997	Codes for the representation of names of countries and their subdivisions — Part 1: Country Codes
ISO 4217:2001	Codes for the representation of currencies and funds.
ISO/IEC 8825:1998	Information technology — Open systems interconnection — Specification of basic encoding rules for abstract syntax notation one (ASN.1).
ISO/IEC 7813:2001 (E)	Identification cards — Financial transaction cards.
ISO/IEC 7816-4:1995 (E)	Information technology — Identification cards — Integrated circuit(s) cards with contacts — Part 4: Interindustry commands for interchange
ISO/IEC 9646:1994	Information technology — Open Systems Interconnection — Conformance testing methodology and framework
ISO/IEC 15145:1997	Information technology — Programming Languages — Forth