American National Standard

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

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

Developed by

Where IT all begins

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

Table of Contents

List of Figures

List of Tables

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 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 Termiual Interface Requirements.* Version 4.0, December 2000.[1]
- 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.

- 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