INTERNATIONAL STANDARD

ISO/IEC 16500-7

First edition
1999-12-15

Information technology — Generic digital audio-visual systems —

Part 7:
Basic security tools

Technologies de l'information — Systèmes audiovisuels numériques génériques —

Partie 7: Outils de sécurité de base

Reference number
ISO/IEC 16500-7:1999(E)

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.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents Page

Foreword vii

Introduction viii

1. Scope 1

2. Normative references 1

3. Definitions 2

4. Acronyms and abbreviations 3

5. Conventions 4

6. Overview of Security System 4

7. Security Tools 5

7.1 S1 Scrambling 5

7.1.1 Scrambled Elements 5

7.1.2 Control Word Synchronization 6

7.2 S2/S3 Authentication 7

7.2.1 Authentication Protocol 7

7.2.2 Syntax of Authentication Messages 8

7.2.3 Key Use 9

7.2.4 Certificates 9

7.2.5 Integration with Protocols for S2 9

7.3 S2/S3 Confidentiality and Integrity 9

7.3.1 Negotiation of Confidentiality and Integrity Algorithms 10

7.3.2 Definition of the SPI value 10

7.3.3 Signaling 10

7.3.4 Replay Protection on S2 10

7.4 S2 Digital Signatures 10

7.5 DSM-CC Commands for S1 Security Management 10

7.5.1 Security Association Configuration 10

7.5.2 Key Retrieval 12

7.6 Secure Download 13

7.6.1 Format of Security DownloadInfoRequest 13

7.6.2 Format of Security DownloadInfoResponse 14

7.6.3 Format of Security Module 14

7.6.4 Download Reasons in DownloadDataResponse 15

7.7 Parental Control 15

7.7.1 Introduction 15

7.7.2 Retrieval Services 15

7.7.3 Distribution Services 15

8. Flows and Protocol Stacks 16

8.1 Sample Flow: Scrambled Video on Demand (Informative) 16

9. Security Interfaces 19

10. Security Interface CA0 20

10.1 Introduction 20

10.2 Additional DAVIC Requirements for CA0 20

10.2.1 Host to Security Device Authentication 20

10.2.2 Security Services 20

11. Profiles/Contours 21

12. Security Interface CA1 21

12.1 Introduction and scope 21

12.1.1 Introduction 21

12.1.2 CA1 reference model 21

12.2 Notation 23

12.3 Physical characteristics of the CA1 security device 23

12.4 Electronic signals and transmission protocols on the CA1 interface 23

12.4.1 Additions and restrictions to ISO/IEC 7816-3 23

12.4.2 Logical channels 24

12.5 CA message format and filter specification 24

12.5.1 CA message mechanism and format 24

12.5.2 Filtering of a CA message 24

12.5.3 Filter specification 25

12.5.4 Filter programming 25

12.5.5 Filter objects 27

12.5.6 Response objects from smart card 31

12.5.7 Filter conditions 32

12.5.8 Further filter requirements 32

12.6 Initialization of the smart card and application 33

12.6.1 Answer-to-Reset 33

12.6.2 Conditional PTS procedure 35

12.6.3 The ATR and/or DIR file 35

12.6.4 Card identification and initialization data 35

12.6.5 Application identification and selection 36

12.6.6 Application-independent card services 37

12.7 Smart card security functions 37

12.7.1 Access conditions 37

12.7.2 Commands and access conditions 38

12.7.3 Password management 39

12.7.4 Authentication 39

12.8 Data structures in the smart card 40

12.8.1 Introduction 40

12.8.2 File organization 40

12.8.3 Data structure headers 42

12.8.4 EF file content 45

12.8.5 Overview of DAVIC data objects 46
12.9 Basic data objects 47
12.9.1 Introduction 47
12.9.2 Application_related_data 47
12.9.3 System_related_data 48
12.9.4 Service_provider_related_data 49
12.9.5 Filtering 49
12.9.6 Parental_rating 50
12.9.7 Entitlement data 50
12.9.8 Response messages 51
12.10 Smart card commands 53
12.10.1 Introduction 53
12.10.2 Coding of the commands 53
12.10.3 Select_file 53
12.10.4 Read_binary 54
12.10.5 Read_record 55
12.10.6 Seek 56
12.10.7 Verify_password 57
12.10.8 Change_password 57
12.10.9 Disable_password 58
12.10.10 Enable_password 59
12.10.11 Write_binary 59
12.10.12 Write_record 60
12.10.13 Update_binary 61
12.10.14 Update_record 61
12.10.15 Get_response 62
12.10.16 Get_data 63
12.10.17 Put_data 64
12.10.18 Get_application_status 65
12.10.19 Perform_security_operation 66
12.10.20 Status Conditions returned by the smart card 66
12.11 Man machine interface 69
12.11.1 Introduction 69
12.11.2 MMI objects 70
12.12 Tag allocation 72
12.12.1 General 72
12.12.2 Tag allocation for DAVIC application 73
13. Additional Resources for the DAVIC CA0 Interface 79
13.1 Host-provided Resources 79
13.1.1 TCP/IP Socket Resource 79
13.1.2 HTML MMI Display 86
13.2 PC card-provided Resources 87
13.2.1 Authentication Support 87
13.2.2 IP Security Support 89

14. Informative Methodology 91

14.1 Procedure 91

14.2 Logical Business Model 91

14.3 Systems Review 92

14.4 Threat Analysis 92

14.4.1 Threat Classes 92

14.4.2 Threats for Content Flow S1 93

14.4.3 Threats for Application Control Flow S2 94

14.5 Risk Assessment 94

14.5.1 S1 Flow 96

14.5.2 S2 Flow 97

14.6 Requirements Resulting from the Risk Analysis 97

14.6.1 S1 Flow 97

14.6.2 S2 Flow 98

14.6.3 Legislatory And Regulatory Requirements 98

14.7 Security Services 99

14.7.1 General Security Services 99

14.8 Security Mechanisms 100

Bibliography 101

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 part of ISO/IEC 16500 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 16500-7 was prepared by DAVIC (Digital Audio-Visual Council) 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.

ISO/IEC 16500 consists of the following parts, under the general title *Information technology — Generic digital audio-visual systems*:

— *Part 1: System reference models and scenarios*

— *Part 2: System dynamics, scenarios and protocol requirements*

— *Part 3: Contours: Technology domain*

— *Part 4: Lower-layer protocols and physical interfaces*

— *Part 5: High and mid-layer protocols*

— *Part 6: Information representation*

— *Part 7: Basic security tools*

— *Part 8: Management architecture and protocols*

— *Part 9: Usage information protocols*

Introduction

ISO/IEC 16500 defines the minimum tools and dynamic behavior required by digital audio-visual systems for end-to-end interoperability across countries, applications and services. To achieve this interoperability, it defines the technologies and information flows to be used within and between the major components of generic digital audio-visual systems. Interoperability between these components and between individual sub-systems is assured through specification of tools and specification of dynamic systems behavior at defined reference points. A reference point can comprise one or more logical (non-physical) information-transfer interfaces, and one or more physical signal-transfer interfaces. A logical interface is defined by a set of information flows and associated protocol stacks. A physical interface is an external interface and is fully defined by its physical and electrical characteristics. Accessible reference points are used to determine and demonstrate compliance of a digital audio-visual subsystem with this international standard.

A summary of each part follows.

ISO/IEC 16500-1 (DAVIC 1.3.1a Part 2) defines the normative digital audio-visual systems technical framework. It provides a vocabulary and a Systems Reference Model, which identifies specific functional blocks and information flows, interfaces and reference points.

ISO/IEC 16500-2 (DAVIC 1.3.1a Part 12) defines system dynamic behavior and physical scenarios. It details the locations of the control functional entities along with the normative protocols needed to support the systems behavior. It is structured as a set of protocol walk-throughs, or "*Application Notes*", that rehearse both the steady state and dynamic operation of the system at relevant reference points using specified protocols. Detailed dynamics are given for the following scenarios: video on demand, switched video broadcast, interactive broadcast, and internet access.

ISO/IEC 16500-3 (DAVIC 1.3.1a Part 14) provides the normative definition of DAVIC Technology Contours. These are strict sets of Applications, Functionalities and Technologies which allow compliance and conformance criteria to be easily specified and assessed. This part of ISO/IEC 16500 contains the full details of two contours. These are the Enhanced Digital Broadcast (EDB) and Interactive Digital Broadcast (IDB). ISO/IEC 16500-3 specifies required technologies and is a mandatory compliance document for contour implementations.

ISO/IEC 16500-4 (DAVIC 1.3.1a Part 8) defines the toolbox of technologies used for lower layer protocols and physical interfaces. The tools specified are those required to digitize signals and information in the Core Network and in the Access Network. Each tool is applicable at one or more of the reference points specified within the Delivery System. In addition a detailed specification is provided of the physical interfaces between the Network Interface Unit and the Set Top Unit and of the physical interfaces used to connect Set Top Boxes to various peripheral devices (digital video recorder, PC, printer). The physical Delivery System mechanisms included are copper pairs, coaxial cable, fiber, HFC, MMDS, LMDS, satellite and terrestrial broadcasting.

ISO/IEC 16500-5 (DAVIC 1.3.1a Part 7) defines the technologies used for high and mid-layer protocols for ISO/IEC 16500 digital audio-visual systems. In particular, this part defines the specific protocol stacks and requirements on protocols at specific interfaces for the content, control and management information flows.

ISO/IEC 16500-6 (DAVIC 1.3.1a Part 9) defines what the user will eventually see and hear and with what quality. It specifies the way in which monomedia and multimedia information types are coded and exchanged. This includes the definition of a virtual machine and a set of APIs to support interoperable exchange of program code. Interoperability of applications is achieved, without specifying the internal design of a set top unit, by a normative Reference Decoder Model which defines specific memory and behavior constraints for content decoding. Separate profiles are defined for different sets of multimedia components.

ISO/IEC 16500-7 (DAVIC 1.3.1a Part 10) defines the interfaces and the security tools required for an ISO/IEC 16500 system implementing security profiles. These tools include security protocols which operate across one or both of the defined conditional access interfaces CA0 and CA1. The interface CA0 is to all security and conditional access functions, including the high speed descrambling functions. The interface CA1 is to a tamper resistant device used for low speed cryptographic processing. This cryptographic processing function is implemented in a smart card.

ISO/IEC 16500-8 (DAVIC 1.3.1a Part 6) specifies the information model used for managing ISO/IEC 16500 systems. In particular, this part defines the managed object classes and their associated characteristics for managing the access network and service-related data in the Delivery System. Where these definitions are taken from existing standards, full reference to the required standards is provided. Otherwise a full description is integrated in the text of this part. Usage-related information model is defined in ISO/IEC 16500-9.

ISO/IEC 16500-9 (DAVIC 1.3.1a Part 11) specifies the interface requirements and defines the formats for the collection of usage data used for billing, and other business-related operations such as customer profile maintenance. It also specifies the protocols for the transfer of Usage Information into and out of the ISO/IEC 16500 digital audio-visual system. In summary, flows of audio, video and audio-visual works are monitored at defined usage data collection elements (e.g. servers, elements of the Delivery System, set-top boxes). Information concerning these flows is then collected, processed and passed to external systems such as billing or a rights administration society via a standardised usage data transfer interface.

Additional Information

ISO/IEC TR 16501 is an accompanying Technical Report. Further architectural and conformance information is provided in other non-normative parts of DAVIC 1.3.1a (1999). A summary of these documents is included here for information.

ISO/IEC TR 16501 (DAVIC 1.3.1a Part 1) provides a detailed listing of the functionalities required by users and providers of digital audio-visual applications and systems. It introduces the concept of a contour and defines the IDB (Interactive Digital Broadcast) and EDB (Enhanced Digital Broadcast) functionality requirements which are used to define the normative contour technology toolsets provided in ISO/IEC 16500-3.

DAVIC 1.3.1a Parts 3, 4 and 5 are DAVIC technical reports. They provide additional architectural and other information for the server, the delivery-system, and the Service Consumer systems respectively. Part 3 defines how to load an application, once created, onto a server and gives information and guidance on the protocols transmitted from the set-top user to the server, and those used to control the set-up and execution of a selected application. Part 4 provides an overview of Delivery Systems and describes instances of specific DAVIC networked service architectures. These include physical and wireless networks. Non-networked delivery (e.g. local storage physical media like discs, tapes and CD-ROMs) are not specified. Part 5 provides a Service Consumer systems architecture and a description of the DAVIC Set Top reference points defined elsewhere in the normative parts of the specification.

DAVIC 1.3.1a Part 13 is a DAVIC technical report, which provides guidelines on how to validate the systems, technology tools and protocols through conformance and / or interoperability testing.

Information technology — Generic digital audio-visual systems — Part 7: Basic security tools

1. Scope

This part of ISO/IEC 16500 deals with security in DAVIC systems. A number of security tools are specified, including security protocols which operate across DAVIC interfaces, as well as two security related interfaces in the STU. These security tools must be implemented in ISO/IEC 16500 systems conforming to the security profiles.

2. Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 16500. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 16500 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau (TSB) maintains a list of currently valid ITU-T Recommendations.

2.1 ISO/IEC and ITU normative references

ISO/IEC 7816-1: 1987, *Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics.*

ISO/IEC 7816-2: 1988, *Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts*.

ISO/IEC 7816-3: 1989, *Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols*.

ISO/IEC 7816-4: 1995, *Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange*.

ISO/IEC 7816-5: 1994, *Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers.*

ISO/IEC 7816-6: 1996, *Identification cards - Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements.*

ISO/IEC 7816-8, *Identification cards - Integrated circuit card(s) with contacts - Part 8: Security related interindustry commands.*

ISO/IEC 8824: 1990, *Information technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1).*

ISO/IEC 8825: 1990, *Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

ISO/IEC 13818-1: 1996, *Information technology - Generic coding of moving pictures and associated audio information: Systems.*

ISO/IEC 13818-6: 1998, *Information technology - Generic coding of moving pictures and associated audio information - Part 6: Extensions for DSM-CC.*

ITU Recommendation X.509, *Information technology - Open System Interconnection - The Directory: Authentication Framework*, Amendment 2, 1996.

ITU Recommendation X.511, Information technology - Open System Interconnection - The Directory: Abstract Service Definition, Amendment 4, 1996.

2.2 Other normative references

CENELEC EN 50221 : 1997, *Common Interface for Conditional Access and other Digital Video Decoder Applications.*

CENELEC R 206-001 : 1997, *Guidelines for the Implementation and Use of the Common Interface for DVB Decoder Applications.*

ETSI ETR 162: 1995, *Digital Video Broadcasting (DVB): Allocation of Service Information (SI) codes for DVB Systems*.

ETSI ETR 332: 1996-11, *Security requirements capture.*

ETSI ETS 300 468: 1997-01, *Digital Video Broadcasting (DVB) - Specification for Service Information (SI) in DVB systems.*

ETSI ETS 300 608: 1997-08, *Digital cellular telecommunication system (Phase 2) - Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface (GSM11.11).*

ETSI prEN 726-3, *Terminal equipment (TE) - Requirements for IC cards and terminals for telecommunication use - Part 3: Application independent card requirements.*

Personal Computer Memory Card International Association, *PC Card Standard - Volume 2: Electrical Specification*, February 1995.

Personal Computer Memory Card International Association, *PC Card Standard - Volume 3: Physical Specification*, February 1995.

Personal Computer Memory Card International Association, *PC Card Standard - Volume 4: Metaformat Specification*, February 1995.