

# ISO/IEC 20060:2010-07 (E)

## Information technology - Open Terminal Architecture (OTA) - Virtual machine

---

<b>Contents</b>		<b>Page</b>
Foreword .....		vi
Introduction .....		vii
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	1
4	Symbols and abbreviated terms .....	5
5	Data types, stack notation and flags .....	6
5.1	Data Types .....	6
5.2	Stack Notation .....	7
5.3	Flags .....	7
6	OTA virtual machine .....	7
6.1	General principles .....	7
6.2	Virtual Machine CPU .....	8
6.2.1	Registers .....	9
6.2.2	Virtual Machine Size and Cells .....	9
6.2.3	Memory .....	9
6.2.4	Stacks .....	10
6.2.5	Frame Mechanism and Usage .....	11
6.2.6	Extensible Memory .....	12
6.2.7	User Variables .....	12
6.3	Virtual Machine Execution Features .....	13
6.4	Arithmetic .....	13
6.5	Exception Handling .....	14
6.6	Resources .....	15
6.7	Programs and Tokens .....	15
7	System Services .....	16
7.1	Time Handling .....	16
7.2	Devices and I/O Services .....	17
7.3	Database Services .....	17
7.3.1	The Database Parameter Block .....	19
7.3.2	Database Instantiation .....	21
7.3.3	Database Exception Handling .....	22
7.4	Language and Message Handling .....	22
7.5	TLV Services .....	23
7.5.1	Basic Principles .....	23
7.5.2	TLV Definitions .....	23
7.5.3	TLV References .....	24
7.6	Hot Card List Management .....	25
7.7	Cryptographic Services .....	25
7.7.1	Modulo Multiplication .....	26
7.7.2	Secure Hash Algorithm (SHA-1) .....	26
7.7.3	Modulo Exponentiation .....	27
7.7.4	Long Shift .....	27
7.7.5	Long Subtract .....	27

7.7.6	Incremental Secure Hash Algorithm (SHA-1)	27
7.7.7	Cyclic Redundancy Check (CRC)	28
7.7.8	DES Key Schedule	28
7.7.9	DES encryption/decryption	28
7.8	Vectored Execution Sockets	28
7.8.1	CSS Functions	29
7.8.2	Socket Security	29
7.8.3	Socket Organisation	29
7.9	Module Handling Services	29
7.9.1	Module Loading by MODEXECUTE	30
7.9.2	Module Loading Procedure	32
7.9.3	Module Loading by MODCARDEXECUTE	35
8	Token Set Definition	37
8.1	Overview	37
8.2	Conventions	37
8.2.1	Number Formats	37
8.2.2	Token Descriptions	38
8.2.3	Branch and Code Offsets	38
8.2.4	Addresses	38
8.3	Data Typing	39
8.4	Token Compression	39
8.4.1	Optimised Data Access	39
8.4.2	Special Procedure Calls	39
8.4.3	Quoting	39
8.5	Prefix Tokens	40
8.6	Stack Manipulation Tokens	41
8.7	Data Access Tokens	43
8.8	Literal Tokens	45
8.9	Address Generation Tokens	46
8.10	Arithmetic Tokens	47
8.11	Relational Tokens	51
8.12	String Tokens	53
8.13	Frame Tokens	56
8.14	Extensible Memory Tokens	58
8.15	Flow of Control Tokens	59
8.15.1	Branch Tokens	59
8.15.2	Call Tokens	60
8.15.3	Loop Tokens	61
8.15.4	Hybrid Tokens	62
8.15.5	Quoting Tokens	63
8.16	Exception Tokens	63
8.17	Date, Time, and Timing Tokens	64
8.18	Generic Device I/O Tokens	64
8.19	Formatted I/O Tokens	68
8.20	Integrated Circuit Card Tokens	69
8.21	Magnetic Stripe Tokens	70
8.22	Socket Tokens	71
8.23	Database Services Tokens	72
8.24	Language and Message Tokens	77
8.25	TLV Tokens	78
8.25.1	TLV Buffer Access	78
8.25.2	TLV Processing	80
8.25.3	TLV Sequence Access	81
8.26	Hot Card List Tokens	82
8.27	Cryptographic Algorithm Token	83
8.28	Module Management Tokens	83
8.29	Operating System Interface Tokens	84
8.30	Miscellaneous Tokens	84
9	Module Delivery Format	85
9.1	Module ID Format	86

<b>9.2</b>	<b>Socket List .....</b>	<b>86</b>
<b>9.3</b>	<b>Relocation Section .....</b>	<b>87</b>
<b>9.4</b>	<b>Module Import List .....</b>	<b>88</b>
<b>9.5</b>	<b>Module Export List .....</b>	<b>88</b>
<b>9.6</b>	<b>Module Procedure List .....</b>	<b>89</b>
<b>Annex A (normative) OTA Token Lists .....</b>		<b>90</b>
<b>Annex B (normative) Exceptions and I/O Return Codes .....</b>		<b>97</b>
<b>Annex C (normative) Device Control .....</b>		<b>101</b>
<b>Annex D (normative) Operating System Calls .....</b>		<b>116</b>
<b>Annex E (normative) Rules for Using a Data Object List (DOL) .....</b>		<b>117</b>
<b>Annex F (informative) System Overview .....</b>		<b>118</b>
<b>Bibliography .....</b>		<b>137</b>