

ISO/IEC TR 15446:2009-03 (E)

Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets

Contents		Page
Foreword		vii
Introduction		viii
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviations	1
5	Purpose and structure of this technical report	2
6	An overview of PPs and STs	3
6.1	Introduction	3
6.2	Audience	3
6.3	The use of PPs and STs	3
6.3.1	Introduction	3
6.3.2	Specification-based purchasing processes	4
6.3.3	Selection-based purchasing processes	7
6.3.4	Other uses of PPs	8
6.4	The PP/ST development process	9
6.5	Reading and understanding PPs and STs	9
6.5.1	Introduction	9
6.5.2	Reading the TOE overview	10
6.5.3	Reading the TOE description	11
6.5.4	Security objectives for the operational environment	12
6.5.5	Reading the conformance claim	12
6.5.6	Conformance to Protection Profiles	13
6.5.7	EALs and other assurance issues	13
6.5.8	Summary	14
6.5.9	Further reading	15
7	Specifying the PP/ST introduction	15
8	Specifying conformance claims	15
9	Specifying the security problem definition	16
9.1	Introduction	16
9.2	Identifying the informal security requirement	18
9.2.1	Introduction	18
9.2.2	Sources of information	18
9.2.3	Documenting the informal requirement	20
9.3	How to identify and specify threats	21
9.3.1	Introduction	21
9.3.2	Deciding on a threat analysis methodology	21
9.3.3	Identifying participants	22
9.3.4	Applying the chosen threat analysis methodology	26
9.3.5	Practical advice	27
9.4	How to identify and specify policies	28

9.5	How to identify and specify assumptions	29
9.6	Finalising the security problem definition	31
10	Specifying the security objectives	32
10.1	Introduction	32
10.2	Structuring the threats, policies and assumptions	34
10.3	Identifying the non-IT operational environment objectives	34
10.4	Identifying the IT operational environment objectives	35
10.5	Identifying the TOE objectives	36
10.6	Producing the objectives rationale	39
11	Specifying extended component definitions	40
12	Specifying the security requirements	43
12.1	Introduction	43
12.2	The security paradigms in ISO/IEC 15408	45
12.2.1	Explanation of the security paradigms and their usage for modelling the security functionality	45
12.2.2	Controlling access to and use of resources and objects	45
12.2.3	User management	49
12.2.4	TOE self protection	50
12.2.5	Securing communication	51
12.2.6	Security audit	52
12.2.7	Architectural requirements	53
12.3	How to specify security functional requirements in a PP or ST	54
12.3.1	How should security functional requirements be selected?	54
12.3.2	Selecting SFRs from ISO/IEC 15408-2	57
12.3.3	How to perform operations on security functional requirements	59
12.3.4	How should the audit requirements be specified?	61
12.3.5	How should management requirements be specified?	62
12.3.6	How should SFRs taken from a PP be specified?	63
12.3.7	How should SFRs not in a PP be specified?	63
12.3.8	How should SFRs not included in Part 2 of ISO/IEC 15408 be specified?	64
12.3.9	How should the SFRs be presented?	64
12.3.10	How to develop the security requirements rationale	65
12.4	How to specify assurance requirements in a PP or ST	66
12.4.1	How should security assurance requirements be selected?	66
12.4.2	How to perform operations on security assurance requirements	67
12.4.3	How should SARs not included in Part 3 of ISO/IEC 15408 be specified in a PP or ST?	67
12.4.4	Security assurance requirements rationale	68
13	The TOE summary specification	68
14	Specifying PP/STs for composed and component TOEs	69
14.1	Composed TOEs	69
14.2	Component TOEs	72
15	Special cases	72
15.1	Low assurance Protection Profiles and Security Targets	72
15.2	Conforming to national interpretations	73
15.3	Functional and assurance packages	73
16	Use of automated tools	73
	Annex A (informative) Example for the definition of an extended component	75
	Bibliography	78
	Index	79