

ISO/IEC TR 15446:2017-10 (E)

Information technology - Security techniques - Guidance for the production of protection profiles and security targets

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	1
5	Purpose and structure of this document	2
6	Overview of PPs and STs	2
6.1	General	2
6.2	Audience	2
6.3	Use of PPs and STs	3
6.3.1	General	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	8
6.4.1	Including stakeholders in the development process	8
6.4.2	Method to develop a PP or ST	9
6.4.3	Evaluation of PPs and STs	9
6.5	Reading and understanding PPs and STs	10
6.5.1	General	10
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	15
6.5.9	Further reading	15
7	Specifying the PP/ST introduction	15
8	Specifying conformance claims	16
9	Specifying the security problem definition	17
9.1	General	17
9.2	Identifying the informal security requirement	18
9.2.1	General	18
9.2.2	Sources of information	19
9.2.3	Documenting the informal requirement	20
9.3	How to identify and specify threats	21
9.3.1	General	21
9.3.2	Deciding on a threat analysis methodology	21
9.3.3	Identifying participants	23

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	Finalizing the security problem definition	31
10	Specifying the security objectives	32
10.1	General	32
10.2	Structuring the threats, policies and assumptions	33
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	35
10.6	Producing the objectives rationale	38
11	Specifying extended component definitions	39
12	Specifying the security requirements	43
12.1	General	43
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	48
12.2.4	TOE self protection	49
12.2.5	Securing communication	50
12.2.6	Security audit	52
12.2.7	Architectural requirements	52
12.3	How to specify security functional requirements in a PP or ST	53
12.3.1	How should security functional requirements be selected?	53
12.3.3	How to perform operations on security functional requirements	58
12.3.4	How should the audit requirements be specified?	60
12.3.5	How should management requirements be specified?	61
12.3.6	How should SFRs taken from a PP be specified?	62
12.3.7	How should SFRs not in a PP be specified?	62
12.3.9	How should the SFRs be presented?	63
12.3.10	How to develop the security requirements rationale	63
12.4	How to specify assurance requirements in a PP or ST	64
12.4.1	How should security assurance requirements be selected?	64
12.4.2	How to perform operations on security assurance requirements	65
PP or ST?	66
12.4.4	Security assurance requirements rationale	66
13	The TOE summary specification	67
14	Specifying PP/STs for composed and component TOEs	67
14.1	Composed TOEs	67
14.2	Component TOEs	70
15	Special cases	71
15.1	Low assurance Protection Profiles and Security Targets	71
15.2	Conforming to national interpretations	71
15.3	Concepts to enhance the flexibility of Protection Profiles	72
15.3.1	Functional and assurance packages	72
15.3.2	Extended packages	72
15.3.3	Conditional security functional and assurance requirements	72
15.3.4	Optional security functional and security assurance requirements	73
16	Use of automated tools	73
Annex A (informative)	Example for the definition of an extended component	75

Annex B (informative) Example for the specification of refinements77
Bibliography79