

INTERNATIONAL STANDARD

ISO/IEC 15408-2

First edition
1999-12-01

iTeh STANDARD PREVIEW

*Technologies de l'information — Techniques de sécurité — Critères
d'évaluation pour la sécurité TI*

Partie 2: Exigences fonctionnelles de sécurité

ISO/IEC 15408-2:1999

<https://standards.iteh.ai/catalog/standards/sist/515c2bf6-f3b8-492c-8790-e8c24aeb826e/iso-iec-15408-2-1999>



Reference number
ISO/IEC 15408-2:1999(E)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 15408-2:1999](https://standards.iteh.ai/catalog/standards/sist/515c2bf6-f3b8-492c-8790-e8c24aeb826e/iso-iec-15408-2-1999)

<https://standards.iteh.ai/catalog/standards/sist/515c2bf6-f3b8-492c-8790-e8c24aeb826e/iso-iec-15408-2-1999>

Contents

1	Scope	1
1.1	Extending and maintaining functional requirements	1
1.2	Organisation of ISO/IEC 15408-2	2
1.3	Functional requirements paradigm	2
2	Security functional components	9
2.1	Overview	9
2.1.1	Class structure	9
2.1.2	Family structure	10
2.1.3	Component structure	11
2.1.4	Permitted functional component operations	13
2.2	Component catalogue	14
2.2.1	Component changes highlighting	15
3	Class FAU: Security audit	17
3.1	Security audit automatic response (FAU_ARP)	18
3.2	Security audit data generation (FAU_GEN)	19
3.3	Security audit analysis (FAU_SAA)	21
3.4	Security audit review (FAU_SAR)	24
3.5	Security audit event selection (FAU_SEL)	26
3.6	Security audit event storage (FAU_STG)	27
4	Class FCO: Communication	31
4.1	Non-repudiation of origin (FCO_NRO)	32
4.2	Non-repudiation of receipt (FCO_NRR)	34
5	Class FCS: Cryptographic support	37
5.1	Cryptographic key management (FCS_CKM)	38
5.2	Cryptographic operation (FCS_COP)	41
6	Class FDP: User data protection	43
6.1	Access control policy (FDP_ACC)	46
6.2	Access control functions (FDP_ACF)	48
6.3	Data authentication (FDP_DAU)	50
6.4	Export to outside TSF control (FDP_ETC)	52
6.5	Information flow control policy (FDP_IFC)	54
6.6	Information flow control functions (FDP_IFF)	56
6.7	Import from outside TSF control (FDP_ITC)	61
6.8	Internal TOE transfer (FDP_ITT)	63
6.9	Residual information protection (FDP_RIP)	66
6.10	Rollback (FDP_ROL)	68
6.11	Stored data integrity (FDP_SDI)	70

6.12	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	72
6.13	Inter-TSF user data integrity transfer protection (FDP_UIT)	73
7	Class FIA: Identification and authentication	77
7.1	Authentication failures (FIA_AFL)	79
7.2	User attribute definition (FIA_ATD)	80
7.3	Specification of secrets (FIA_SOS)	81
7.4	User authentication (FIA_UAU)	83
7.5	User identification (FIA_UID)	88
7.6	User-subject binding (FIA_USB)	90
8	Class FMT: Security management	91
8.1	Management of functions in TSF (FMT_MOF)	93
8.2	Management of security attributes (FMT_MSA)	94
8.3	Management of TSF data (FMT_MTD)	97
8.4	Revocation (FMT_REV)	99
8.5	Security attribute expiration (FMT_SAE)	100
8.6	Security management roles (FMT_SMR)	101
9	Class FPR: Privacy	105
9.1	Anonymity (FPR_ANO)	106
9.2	Pseudonymity (FPR_PSE)	108
9.3	Unlinkability (FPR_UNL)	110
9.4	Unobservability (FPR_UNO)	111
10	Class FPT: Protection of the TSF	115
10.1	Underlying abstract machine test (FPT_AMT)	118
10.2	Fail secure (FPT_FLS)	119
10.3	Availability of exported TSF data (FPT_ITA)	120
10.4	Confidentiality of exported TSF data (FPT_ITC)	121
10.5	Integrity of exported TSF data (FPT_ITI)	122
10.6	Internal TOE TSF data transfer (FPT_ITT)	124
10.7	TSF physical protection (FPT_PHP)	127
10.8	Trusted recovery (FPT_RCV)	130
10.9	Replay detection (FPT_RPL)	133
10.10	Reference mediation (FPT_RVM)	134
10.11	Domain separation (FPT_SEP)	135
10.12	State synchrony protocol (FPT_SSP)	137
10.13	Time stamps (FPT_STM)	139
10.14	Inter-TSF TSF data consistency (FPT_TDC)	140
10.15	Internal TOE TSF data replication consistency (FPT_TRC)	141
10.16	TSF self test (FPT_TST)	142
11	Class FRU: Resource utilisation	145
11.1	Fault tolerance (FRU_FLT)	146
11.2	Priority of service (FRU_PRS)	148
11.3	Resource allocation (FRU_RSA)	150
12	Class FTA: TOE access	153
12.1	Limitation on scope of selectable attributes (FTA_LSA)	154

12.2	Limitation on multiple concurrent sessions (FTA_MCS)	155
12.3	Session locking (FTA_SSL)	157
12.4	TOE access banners (FTA_TAB)	160
12.5	TOE access history (FTA_TAH)	161
12.6	TOE session establishment (FTA_TSE)	162
13	Class FTP: Trusted path/channels	163
13.1	Inter-TSF trusted channel (FTP_ITC)	164
13.2	Trusted path (FTP_TRP)	166
Annex A	Security functional requirements application notes	169
A.1	Structure of the notes	169
A.1.1	Class structure	169
A.1.2	Family structure	170
A.1.3	Component structure	171
A.2	Dependency table	172
Annex B	Functional classes, families, and components	179
Annex C	Security audit (FAU)	181
C.1	Security audit automatic response (FAU_ARP)	183
C.2	Security audit data generation (FAU_GEN)	184
C.3	Security audit analysis (FAU_SAA)	187
C.4	Security audit review (FAU_SAR)	192
C.5	Security audit event selection (FAU_SEL)	194
C.6	Security audit event storage (FAU_STG)	195
Annex D	Communication (FCO)	199
D.1	Non-repudiation of origin (FCO_NRO)	200
D.2	Non-repudiation of receipt (FCO_NRR)	203
Annex E	Cryptographic support (FCS)	207
E.1	Cryptographic key management (FCS_CKM)	209
E.2	Cryptographic operation (FCS_COP)	212
Annex F	User data protection (FDP)	215
F.1	Access control policy (FDP_ACC)	220
F.2	Access control functions (FDP_ACF)	222
F.3	Data authentication (FDP_DAU)	225
F.4	Export to outside TSF control (FDP_ETC)	227
F.5	Information flow control policy (FDP_IFC)	229
F.6	Information flow control functions (FDP_IFF)	232
F.7	Import from outside TSF control (FDP_ITC)	238
F.8	Internal TOE transfer (FDP_ITT)	241
F.9	Residual information protection (FDP_RIP)	245
F.10	Rollback (FDP_ROL)	247
F.11	Stored data integrity (FDP_SDI)	249
F.12	Inter-TSF user data confidentiality transfer protection (FDP_UCT)	251
F.13	Inter-TSF user data integrity transfer protection (FDP_UIT)	252

Annex G	Identification and authentication (FIA)	255
G.1	Authentication failures (FIA_AFL)	257
G.2	User attribute definition (FIA_ATD)	259
G.3	Specification of secrets (FIA_SOS)	260
G.4	User authentication (FIA_UAU)	262
G.5	User identification (FIA_UID)	266
G.6	User-subject binding (FIA_USB)	267
Annex H	Security management (FMT)	269
H.1	Management of functions in TSF (FMT_MOF)	271
H.2	Management of security attributes (FMT_MSA)	273
H.3	Management of TSF data (FMT_MTD)	276
H.4	Revocation (FMT_REV)	278
H.5	Security attribute expiration (FMT_SAE)	279
H.6	Security management roles (FMT_SMR)	280
Annex I	Privacy (FPR)	283
I.1	Anonymity (FPR_ANO)	285
I.2	Pseudonymity (FPR_PSE)	287
I.3	Unlinkability (FPR_UNL)	292
I.4	Unobservability (FPR_UNO)	294
Annex J	Protection of the TSF (FPT)	299
J.1	Underlying abstract machine test (FPT_AMT)	303
J.2	Fail secure (FPT_FLS)	305
J.3	Availability of exported TSF data (FPT_ITA)	306
J.4	Confidentiality of exported TSF data (FPT_ITC)	307
J.5	Integrity of exported TSF data (FPT_ITI)	308
J.6	Internal TOE TSF data transfer (FPT_ITT)	310
J.7	TSF physical protection (FPT_PHP)	312
J.8	Trusted recovery (FPT_RCV)	314
J.9	Replay detection (FPT_RPL)	317
J.10	Reference mediation (FPT_RVM)	318
J.11	Domain separation (FPT_SEP)	319
J.12	State synchrony protocol (FPT_SSP)	321
J.13	Time stamps (FPT_STM)	322
J.14	Inter-TSF TSF data consistency (FPT_TDC)	323
J.15	Internal TOE TSF data replication consistency (FPT_TRC)	324
J.16	TSF self test (FPT_TST)	325
Annex K	Resource utilisation (FRU)	327
K.1	Fault tolerance (FRU_FLT)	328
K.2	Priority of service (FRU_PRS)	330
K.3	Resource allocation (FRU_RSA)	331
Annex L	TOE access (FTA)	333
L.1	Limitation on scope of selectable attributes (FTA_LSA)	334
L.2	Limitation on multiple concurrent sessions (FTA_MCS)	335
L.3	Session locking (FTA_SSL)	336
L.4	TOE access banners (FTA_TAB)	338

L.5	TOE access history (FTA_TAH)	339
L.6	TOE session establishment (FTA_TSE)	340
Annex M	Trusted path/channels (FTP)	341
M.1	Inter-TSF trusted channel (FTP_ITC)	342
M.2	Trusted path (FTP_TRP)	343

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC 15408-2:1999](https://standards.iteh.ai/catalog/standards/sist/515c2bf6-f3b8-492c-8790-e8c24aeb826e/iso-iec-15408-2-1999)

<https://standards.iteh.ai/catalog/standards/sist/515c2bf6-f3b8-492c-8790-e8c24aeb826e/iso-iec-15408-2-1999>

List of Figures

Figure 1.1 - Security functional requirements paradigm (Monolithic TOE)	3
Figure 1.2 - Diagram of security functions in a distributed TOE	4
Figure 1.3 - Relationship between user data and TSF data	7
Figure 1.4 - Relationship between “authentication data” and “secrets”	8
Figure 2.1 - Functional class structure	9
Figure 2.2 - Functional family structure	10
Figure 2.3 - Functional component structure	12
Figure 2.4 - Sample class decomposition diagram	15
Figure 3.1 - Security audit class decomposition	17
Figure 4.1 - Communication class decomposition	31
Figure 5.1 - Cryptographic support class decomposition	37
Figure 6.1 - User data protection class decomposition	44
Figure 6.2 - User data protection class decomposition (cont.)	45
Figure 7.1 - Identification and authentication class decomposition	78
Figure 8.1 - Security management class decomposition	92
Figure 9.1 - Privacy class decomposition	105
Figure 10.1 - Protection of the TSF class decomposition	116
Figure 10.2 - Protection of the TSF class decomposition (Cont.)	117
Figure 11.1 - Resource utilisation class decomposition	145
Figure 12.1 - TOE access class decomposition	153
Figure 13.1 - Trusted path/channels class decomposition	163
Figure A.1 - Functional class structure	169
Figure A.2 - Functional family structure for application notes	170
Figure A.3 - Functional component structure	171
Figure C.1 - Security audit class decomposition	182
Figure D.1 - Communication class decomposition	199
Figure E.1 - Cryptographic support class decomposition	207
Figure F.1 - User data protection class decomposition	217
Figure F.2 - User data protection class decomposition (cont.)	218
Figure G.1 - Identification and authentication class decomposition	256
Figure H.1 - Security management class decomposition	270
Figure I.1 - Privacy class decomposition	283
Figure J.1 - Protection of the TSF class decomposition	300
Figure J.2 - Protection of the TSF class decomposition (Cont.)	301
Figure K.1 - Resource utilisation class decomposition	327
Figure L.1 - TOE access class decomposition	333
Figure M.1 - Trusted path/channels class decomposition	341

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.

International Standard ISO/IEC 15408-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with Common Criteria Project Sponsoring Organisations. The identical text of ISO/IEC 15408-2 is published by the Common Criteria Project Sponsoring Organisations as *Common Criteria for Information Technology Security Evaluation*. Additional information on the Common Criteria Project and contact information on its Sponsoring Organisations is provided in Annex A of ISO/IEC 15408-1.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

- *Part 1: Introduction and general model*
- *Part 2: Security functional requirements*
- *Part 3: Security assurance requirements*

Annexes A to M of this part of ISO/IEC 15408 are for information only.

This LEGAL NOTICE has been placed in all Parts of ISO/IEC 15408 by request:

The seven governmental organisations (collectively called “the Common Criteria Project Sponsoring Organisations”) identified in ISO/IEC 15408-1 Annex A, as the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluation, Parts 1 through 3 (called the “CC”), hereby grant non-exclusive license to ISO/IEC to use the CC in the development of the ISO/IEC 15408 international standard. However, the Common Criteria Project Sponsoring Organisations retain the right to use, copy, distribute, or modify the CC as they see fit.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15408-2:1999

<https://standards.iteh.ai/catalog/standards/sist/515c2bf6-f3b8-492c-8790-e8c24aeb826e/iso-iec-15408-2-1999>

Information technology — Security techniques — Evaluation criteria for IT security —

Part 2: Security functional requirements

1 Scope

Security functional components, as defined in this part of ISO/IEC 15408, are the basis for the TOE IT security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction with the TOE (i.e. inputs, outputs) or by the TOE's response to stimulus.

Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organisational security policies and assumptions.

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT systems and products. ISO/IEC 15408-1 clause 3 provides additional information on the target audience of ISO/IEC 15408, and on the use of the standard by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

- Consumers who use ISO/IEC 15408-2 when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1 subclause 4.3 provides more detailed information on the relationship between security objectives and security requirements.
- Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in this part of ISO/IEC 15408. They can also use the contents of this part of ISO/IEC 15408 as a basis for further defining the TOE security functions and mechanisms that comply with those requirements.
- Evaluators, who use the functional requirements defined in this part of ISO/IEC 15408 in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use this part of ISO/IEC 15408 to assist in determining whether a given TOE satisfies stated requirements.

1.1 Extending and maintaining functional requirements

ISO/IEC 15408 and the associated security functional requirements described herein are not meant to be a definitive answer to all the problems of IT security. Rather, the standard offers a set of well understood security functional requirements that can be used to create trusted products or systems

reflecting the needs of the market. These security functional requirements are presented as the current state of the art in requirements specification and evaluation.

This part of ISO/IEC 15408 does not presume to include all possible security functional requirements but rather contains those that are known and agreed to be of value by the ISO/IEC 15408-2 authors at the time of release.

Since the understanding and needs of consumers may change, the functional requirements in this part of ISO/IEC 15408 will need to be maintained. It is envisioned that some PP/ST authors may have security needs not (yet) covered by the functional requirement components in ISO/IEC 15408-2. In those cases the PP/ST author may choose to consider using functional requirements not taken from the standard (referred to as extensibility), as explained in Annexes B and C of ISO/IEC 15408-1.

1.2 Organisation of ISO/IEC 15408-2

Clause 1 is the introductory material for ISO/IEC 15408-2.

Clause 2 introduces the catalogue of ISO/IEC 15408-2 functional components while clauses 3 through 13 describe the functional classes.

Annex A provides additional information of interest to potential users of the functional components including a complete cross reference table of the functional component dependencies.

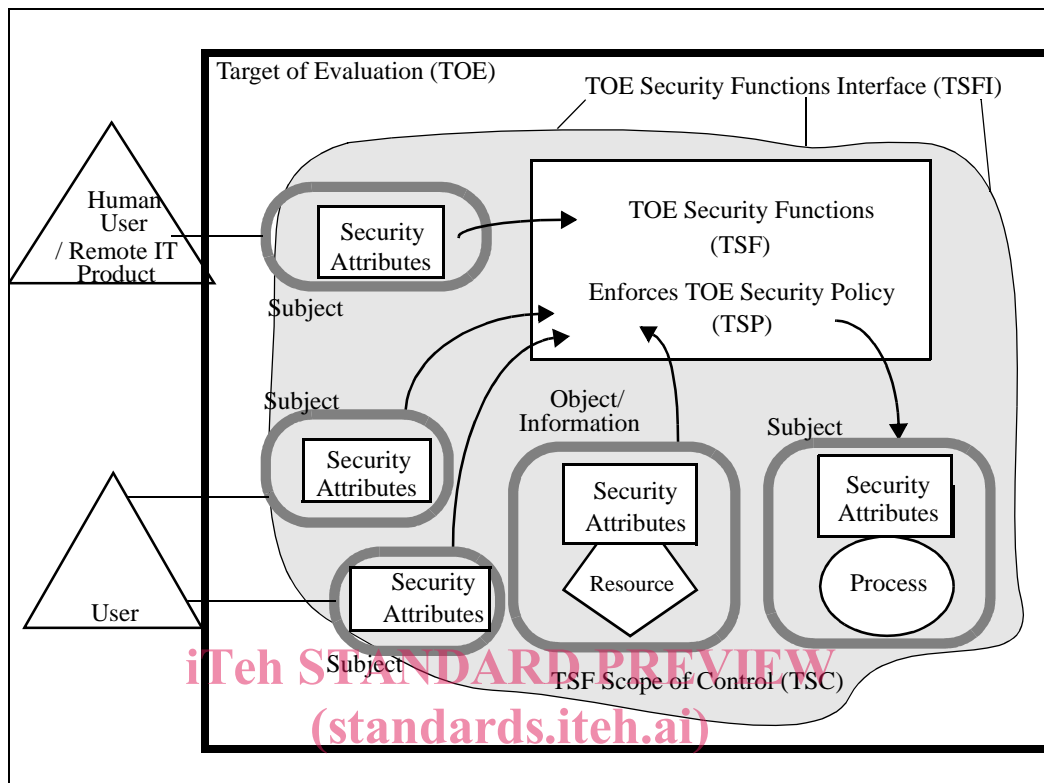
Annexes B through M provide the application notes for the functional classes. They are a repository for informative supporting material for the users of this part of ISO/IEC 15408, which may help them to apply relevant operations and select appropriate audit or documentation information.

Those who author PPs or STs should refer to Clause 2 of ISO/IEC 15408-1 for relevant structures, rules, and guidance:

- ISO/IEC 15408-1, clause 2 defines the terms used in ISO/IEC 15408.
- ISO/IEC 15408-1, Annex B defines the structure for PPs.
- ISO/IEC 15408-1, Annex C defines the structure for STs.

1.3 Functional requirements paradigm

This subclause describes the paradigm used in the security functional requirements of this part of ISO/IEC 15408. Figures 1.1 and 1.2 depict some of the key concepts of the paradigm. This subclause provides descriptive text for those figures and for other key concepts not depicted. Key concepts discussed are highlighted in bold/italics. This subclause is not intended to replace or supersede any of the terms found in the ISO/IEC 15408 glossary in ISO/IEC 15408-1, clause 2.



ISO/IEC 15408-2:1999
 Figure 1.1 - Security functional requirements paradigm (Monolithic TOE)

This part of ISO/IEC 15408 is a catalogue of security functional requirements that can be specified for a **Target of Evaluation (TOE)**. A TOE is an IT product or system (along with user and administrator guidance documentation) containing resources such as electronic storage media (e.g. disks), peripheral devices (e.g. printers), and computing capacity (e.g. CPU time) that can be used for processing and storing information and is the subject of an evaluation.

TOE evaluation is concerned primarily with ensuring that a defined **TOE Security Policy (TSP)** is enforced over the TOE resources. The TSP defines the rules by which the TOE governs access to its resources, and thus all information and services controlled by the TOE.

The TSP is, in turn, made up of multiple **Security Function Policies (SFPs)**. Each SFP has a scope of control, that defines the subjects, objects, and operations controlled under the SFP. The SFP is implemented by a **Security Function (SF)**, whose mechanisms enforce the policy and provide necessary capabilities.

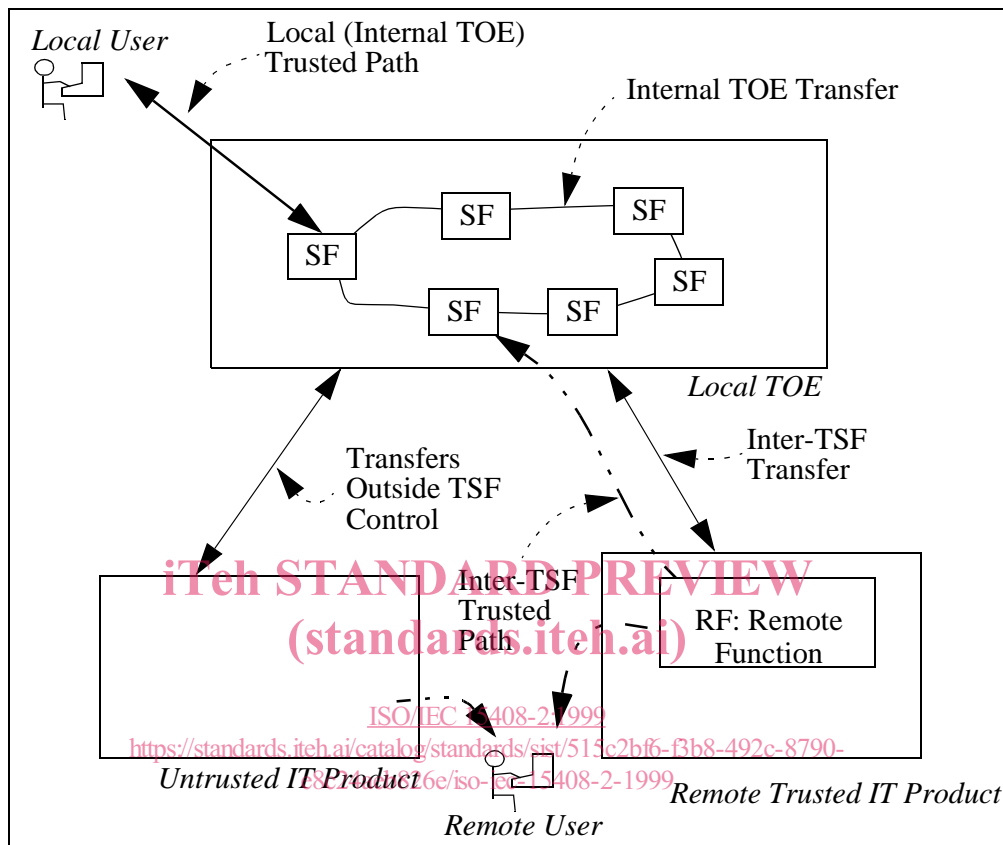


Figure 1.2 - Diagram of security functions in a distributed TOE

Those portions of a TOE that must be relied on for the correct enforcement of the TSP are collectively referred to as the **TOE Security Functions (TSF)**. The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement.

A **reference monitor** is an abstract machine that enforces the access control policies of a TOE. A **reference validation mechanism** is an implementation of the reference monitor concept that possesses the following properties: tamperproof, always invoked, and simple enough to be subjected to thorough analysis and testing. The **TSF** may consist of a reference validation mechanism and/or other security functions necessary for the operation of the TOE.

The TOE may be a monolithic product containing hardware, firmware, and software.

Alternatively a TOE may be a distributed product that consists internally of multiple separated parts. Each of these parts of the TOE provides a particular service for the TOE, and is connected to the other parts of the TOE through an **internal communication channel**. This channel can be as small as a processor bus, or may encompass a network internal to the TOE.

When the TOE consists of multiple parts, each part of the TOE may have its own part of the TSF which exchanges user and TSF data over internal communication channels with other parts of the TSF. This interaction is called *internal TOE transfer*. In this case the separate parts of the TSF abstractly form the composite TSF, which enforces the TSP.

TOE interfaces may be localised to the particular TOE, or they may allow interaction with other IT products over *external communication channels*. These external interactions with other IT products may take two forms:

- a) The security policy of the ‘remote trusted IT product’ and the TSP of the local TOEs have been administratively coordinated and evaluated. Exchanges of information in this situation are called *inter-TSF transfers*, as they are between the TSFs of distinct trusted products.
- b) The remote IT product may not be evaluated, indicated in Figure 1.2 as ‘untrusted IT product’, therefore its security policy is unknown. Exchanges of information in this situation are called *transfers outside TSF control*, as there is no TSF (or its policy characteristics are unknown) on the remote IT product.

The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP is called the *TSF Scope of Control (TSC)*. The TSC encompasses a defined set of interactions based on subjects, objects, and operations within the TOE, but it need not encompass all resources of a TOE.

The set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which resources are accessed that are mediated by the TSF, or information is obtained from the TSF, is referred to as the *TSF Interface (TSFI)*. The TSFI defines the boundaries of the TOE functions that provide for the enforcement of the TSP.

Users are outside of the TOE, and therefore outside of the TSC. However, in order to request that services be performed by the TOE, users interact with the TOE through the TSFI. There are two types of users of interest to the ISO/IEC 15408-2 security functional requirements: *human users* and *external IT entities*. Human users are further differentiated as *local human users*, meaning they interact directly with the TOE via TOE devices (e.g. workstations), or *remote human users*, meaning they interact indirectly with the TOE through another IT product.

A period of interaction between users and the TSF is referred to as a user *session*. Establishment of user sessions can be controlled based on a variety of considerations, for example: user authentication, time of day, method of accessing the TOE, and number of allowed concurrent sessions per user.

This part of ISO/IEC 15408 uses the term *authorised* to signify a user who possesses the rights and/or privileges necessary to perform an operation. The term *authorised user*, therefore, indicates that it is allowable for a user to perform an operation as defined by the TSP.

To express requirements that call for the separation of administrator duties, the relevant ISO/IEC 15408-2 security functional components (from family FMT_SMR) explicitly state that administrative *roles* are required. A role is a pre-defined set of rules establishing the allowed interactions between a user and the TOE. A TOE may support the definition of any number of roles. For example, roles related to the secure operation of a TOE may include “Audit Administrator” and “User Accounts Administrator”.