Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2007/43

4 May 2007

Version 1.0

Amendment Record

Version	Date	Description
1.0	04/05/2007	Public release.

Executive Summary

1 Datacryptor 2000 is a product that is designed to provide data confidentiality. It operates in encrypting/decrypting pairs at the boundary of separate secure domains, and ensures point-to-point confidentiality of data over an insecure domain. Datacryptor 2000 is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Thales e-Security Ltd's Datacryptor 2000, to the Common Criteria (CC) evaluation assurance level EAL 4. The report concludes that the product has met the target assurance level of EAL 4 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by LogicaCMG and was completed on 30 April 2007.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that users ensure that the requirements concerning the operational environment are fulfilled and the relevant guidance documentation is followed. While security claims have not been made regarding the following functionality, the ACA recommends that users:

a) determine that the sensitivity of the motion sensor of the TOE is satisfactory before relying upon its security functionality.

b) considering using the SNMP and RIP protocols, configure these protocols securely to ensure that potentially sensitive configuration information is not exposed to the insecure domain.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1], and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Datacryptor 2000, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 4; and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Datacryptor 2000: • part number 1600x320 • sub-part numbers 1600A321 Rev 5-8, 1600B321 Rev 6, 1600E321 Rev 7. Datacryptor Advanced Performance (DCAP): • part numbers 1600A371, 1600C371, 1600L371, 1600M371 • sub-part numbers 1600A372 Rev 3, 1600L372 Rev 1, 1600M372 Rev 1.
Software Version	Datacryptor 2000 Application Software 3.41 Datacryptor Advanced Performance Application Software 3.511

Security Target	Datacryptor 2000 Security Target Version 1
Evaluation Level	EAL 4
Evaluation Technical Report	Thales Datacryptor 2000 and Datacryptor Advanced Performance Evaluation Technical Report, Issue 1.0, 30 April 2007
Criteria	CC Version 2.1, August 1999, with interpretations as of 14 March 2002.
Methodology	CEM-99/045 Version 1.0, August 1999, with interpretations as of 14 March 2002.
Conformance	CC Part 2 Conformant CC Part 3 Conformant
Developer	Thales e-Security Ltd
Evaluation Facility	LogicaCMG

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is the Datacryptor 2000 developed by Thales e-Security Ltd. The TOE is comprised of two variants: the Datacryptor 2000 and the Datacryptor Advanced Performance. These two variants will be referred to as DC2K and DCAP, respectively. Note, however, that all references to DC2K also refer to the DCAP unless stated otherwise.

12 The TOE's primary role is to provide data confidentiality. It operates in encrypting/decrypting pairs at the boundary of separate secure domains, and ensures point-to-point confidentiality of data over an insecure domain. Several different network protocols are within scope of the evaluation including link, frame relay and IP. The DCAP only includes the IP protocol within the scope of the evaluation.

13 The TOE provides a secure soft-upgrade capability to change the network protocol and cryptographic algorithms supported. The DC2K uses public key cryptography techniques to minimise the administrative overhead of key management and implements sophisticated measures to resist physical attack in order to safeguard key material and sensitive algorithms.

2.3 Security Policy

14 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP model describes four security policies for the TOE that correspond to the security functional requirements detailed in the Security Target (Ref [1]). These security policies, along with their corresponding security functional requirements, are as follows:

a) **Data Authentication**: The TOE authenticates data (e.g. algorithms and key certificates) by verifying digital signatures on the data. The TOE will authenticate a data object if and only if it is properly signed. This TSP corresponds to the SFRs FCS_CKM.2, and FCS_COP.1.

b) **Key (DEK) Generation**: Two units must establish a shared DEK (Data Encryption Key) in order to communicate encrypted data with each other. The model of this policy classifies the system state as a collection of DC2Ks and the generated KEKs (Key Encryption Key) that they contain. The two units can establish a shared DEK securely if and only if they contain the same KEK. This TSP corresponds to the SFRs FCS_CKM.1, and FCS_CKM.2.

c) **Data Encryption**: Secure encryption of data is defined as a property of an encryption system such that, when the mode of the encryption system is set to encrypt, the data that is output by the encryption system is always encrypted. This TSP corresponds to the SFRs FCS_CKM.2, and FCS_COP.1.

d) **Physical Security:** If temperature, power, and the tamper states of the enclosure are outside acceptable levels then an alarm is raised and sensitive data is erased. This TSP corresponds to the SFR FPT_PHP.3.

2.4 TOE Architecture

15 The TOE consists of the following major architectural components:

a) **SGSS Application:** The Secure Generic Sub-System (SGSS) application runs on the SGSS. It consists of a secure bootstrap program that verifies that the DC2K application or another bootstrap version has been signed by the private key of the manufacturer. If the verification fails, the application will not load.

b) **SGSS Hardware:** The SGSS hardware provides a number of functions including a random number generator and alarm circuitry. The SGSS operates as a protection mechanism for the TOEs sensitive data, including keys and algorithms. It provides: resistance to physical intrusion of the SGSS; attacks requiring high and low voltage levels; temperature extreme attacks; and motion sensors. When an alarm is triggered, the voltage supply rails to all devices containing sensitive information are grounded causing them to lose their contents.

c) **DC2K Application:** The DC2K application is responsible for several critical functions including the cryptographic authentication of the key exchange algorithms; encryption algorithm; Certificate Authorities; and Key Exchange Algorithm Keysets.

d) **Key Exchange Algorithm:** The key exchange algorithm used is a hybrid of the Diffie-Hellman algorithm. It allows two TOEs to securely establish a common Key Encryption Key (KEK).

e) **Encryption Algorithm:** Once a KEK has been agreed, both TOE's generate a shared Data Encryption Key (DEK). Once the DEK has been agreed, the encryption algorithm will be used to encrypt and decrypt user data.

16 Further information on the TOE architecture is provided in the Security Target (Ref [1]).

2.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

18 The TOE includes the following communication protocols:

a) Datacryptor 2000: Link, Frame Relay and IP5 (5Mb);

b) Datacryptor Advanced Performance: IP10 (10Mb) and IP100 (10/100Mb).

19 The TOE includes the following cryptographic algorithms:

a) Key Exchange Algorithms:

i) Diffie-Hellman (ANSI X9.42 Hybrid1).

b) Data Encryption Algorithms:

    - i) Triple DES (FIPS PUB 46-3); and
    - ii) AES 128, 256 (FIPS PUB 197).
- c) Data Authentication Algorithm:
    - i) DSA (FIPS 186-2).
- d) Data Hashing Algorithms:
    - i) SHA-1 (FIPS 180-2).

20 The TOE provides the following evaluated security functionality:

- a) Cryptographic Key Generation;
- b) Cryptographic Key Distribution;
- c) Cryptographic Operation; and
- d) Resistance to Physical Attack.

2.5.2 Non-evaluated Functionality

21 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information and Technology Security Manual (ACSI 33) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

22 The functions and services that have not been included as part of the evaluation are provided below:

- a) Use of communication ports, other than in respect of the cryptographic protection given to user traffic. For example, remote monitoring via the network port and using network management utilities via the network port;
- b) Management centre software;
- c) Hot standby functionality;
- d) Remote unit management;
- e) Data Encryption Algorithm: AES 192;
- f) RoHS compliant version;

g) Motion sensor alarm;

h) Erase button;

i) For the DC2K the following communication protocols are excluded:

    i) Link/Channelised E1 or T1;

    ii) Frame Relay E1;

    iii) X.25; and

    iv) IP – Trunk mode.

j) For the DCAP, the Link E3/T3 communication protocol is excluded.

2.6 Usage

2.6.1 Evaluated Configuration

23 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configurations. Australian Government users should refer to ACSI 33 (Ref [2]) to ensure that configurations meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

24 The TOE consists of a number of different builds of the DC2K and DCAP. Both the hardware and software are uniquely identified.

25 Datacryptor 2000:

a) part number 1600x320

b) sub-part numbers 1600A321 Rev 5-8, 1600B321 Rev 6, 1600E321 Rev 7.

26 Datacryptor Advanced Performance:

a) part numbers 1600A371, 1600C371, 1600L371, 1600M371

b) sub-part numbers 1600A372 Rev 3, 1600L372 Rev 1, 1600M372 Rev 1.

27 Datacryptor 2000 Application Software 3.41

28 Datacryptor Advanced Performance Application Software 3.511

29 Evaluation to include the following communications protocols:

a) Datacryptor 2000: Link, Frame Relay and IP5 (5Mb)

b) Datacryptor Advanced Performance: IP10 (10Mb) and IP100 (10/100Mb).

30 TOE Cryptographic Algorithms:

a) Key Exchange Algorithm: Diffie-Hellman (ANSI X9.42 Hybrid1);

b) Data Encryption Algorithms:

i) Triple DES (FIPS PUB 46-3);

ii) AES 128, 256 (FIPS PUB 197).

c) Data Authentication Algorithm: DSA (FIPS PUB 186-2);

d) Data Hashing Algorithm: SHA-1 (FIPS PUB 180-2).

31 While the motion sensor alarm was not included in the scope of the evaluation, the Security Target recommends that it is enabled where theft of the TOE is a threat (Ref [1]). Further information regarding the reliability of the motion sensor during testing is provided in Section 3.3.

32 The TOE includes functionality to support common network management protocols such as SNMP and RIP. This functionality is not enabled by default, however, if it is required then it is important that these protocols are configured so as to not allow potentially sensitive configuration information to be exposed to the insecure domain.

2.6.2 Delivery procedures

33 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

34 The following is an overview of the process that must be followed by a customer to receive the TOE in a secure manner:

a) Submit a purchase order to a Thales sales representative;

b) A Datacryptor 2000 is sent to the customer by Thales, packaged in cartons sealed with Thales tamper-evident tape, using a courier selected from an approved suppliers list. Also in the box with the unit are the following:

i) Power supply;

ii) Keys;

iii) Product Release Note;

iv) Quick start guide.

v) Delivery Note – signed by an authorised signatory prior to despatch (detailing customer name, contact details, courier, date of dispatch, quantity, description of products, serial numbers of the units sent);

vi) Certificate of conformance (if required);

vii) Export Licence (if required).

c) The Datacryptor 2000 is not sent with CDs as standard, but they can be ordered by the client. This is so that clients can order one set of manuals to support multiple units. The product CD contains the following:

i) DC2K Element Manager;

ii) DC2K Manuals;

iii) DC2K Embedded Software.

d) DHL's shipment system (Connect) allows Thales to forward the full shipment details by email to the Customer, Sales Person or whoever provides their email address and is connected to the shipment.

2.6.3 Determining the Evaluated Configuration

35 Purchasers can verify that they have received the evaluated product by doing the following:

a) Check the product description on the delivery note;

b) Check that the courier packaging has not been tampered with;

c) Check the model and part numbers on the Datacryptor unit;

d) Check the label on the software disks; these identify the product as Datacryptor 2000 or Datacryptor AP and give the version number of the software (3.41 for the DC2K and 3.511 for the DCAP);

e) Contact Thales with the Serial Number of the unit received and ask them to confirm that the box received is within the range of acceptable hardware builds for the TOE.

36 If the unit received contains anything indicating that it is RoHS compliant then it is not the evaluated version of the product.

2.6.4 Documentation

37 It is important that the TOE is used in accordance with guidance documentation in order to ensure the secure usage. A selection of the following documentation is provided with the TOE based upon the variant purchased:

a) DataCryptor 2000 Commercial Version User Manual, 1270A357 Issue 002, Thales e-Security, June 2003, (Ref [3]);

b) DataCryptor 2000 Quick-Start Guide, 1270A363 Issue 001, Thales e-Security, 2002 (Ref [4]);

c) DataCryptor 2000 Release 3.4.1 Release Note (Commercial), 1270A370 Issue 2, 22 July 2003 (Ref [5]);

d) DataCryptor 2000 IP, Link, Channelised Link or Frame Relay Network Encryptor – Security Operating Procedures, 1270A461 Issue 001, Thales e-Security, November 2006 (Ref [6]);

e) DataCryptorAP Commercial Version User Manual, 1270A374 Issue 002, Thales e-Security, July 2004 (Ref [7]);

f) Datacryptor AP Quick Start Guide, 1270A378 Issue 001, Thales e-Security (Ref [8]);

g) DataCryptor AP 100Mbps-IP Release Note AES/3DES 3.511 (Commercial), 1270A391 Issue 7, 26 July 2004 (Ref [9]);

h) DataCryptor AP IP Network Encryptor – Security Operating Procedures, 1270A456 Issue 003, Thales e-Security, December 2006 (Ref [10]).

2.6.5 Secure Usage

38 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

39 A brief overview of the assumptions are as follows:

a) Appropriate policies exist with regard to:

   i) The choice of key lifetime;

   ii) Enabling of temperature and motion sensors;

   iii) The usage of the erase button; and

   iv) Action to be taken in the event of suspected tampering, loss or theft of the TOE.

b) The secure environment is protected to a suitable level;

c) All sensitive data is transmitted through the TOE;

d) A suitable mode of operation (e.g. encrypt mode) is applied to sensitive data passing through the TOE;

e) Physical security measures are applied to information within the secure domain. This includes:

   i) key material held externally to the TOE;

   ii) key exchange or encryption algorithms held externally to the unit;

   iii) the TOE while keyed; and

   iv) the management centre.

f) Where the TOE management is required, a separate connection is made to one of the TOE two management ports, and that neither management port is connected to the host network;

g) Where secret keys or sensitive algorithms are to be loaded into the TOE, this must be done over a physically secured network or link;

h) Administrative personnel are trusted to handle key material, sensitive algorithms, and configure the TOE appropriately; and

i) Administrative personnel have the necessary skill to operate the standard Windows application and that they have read the appropriate user manuals.

40 Section 6.1 of the Security Target (Ref [1]) provides a full description of the assumptions.

Chapter 3 - Evaluation

3.1 Overview

41 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

42 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [11], [12], [13]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [14]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [15], [16], [17], [18]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [19]) were also upheld.

3.3 Functional Testing

43 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

44 The evaluators repeated approximately 36% of the developer's tests. This sample was chosen to:

a) Include some testing of all security functions and all variants of the TOE;

b) Focus on the key security function of the TOE, that is data encryption;

c) Provide assurance that the cryptographic algorithms are implemented correctly in the TOE.

45 The evaluators found that in approximately one third of the DC2K units tested that the motion sensor alarm did not activate as expected. The units that failed this test did not respond when carefully turned upside down or given one or two sharp taps.

46 This issue is noted in the Security Target (Ref [1]) with a caveat concerning the sensitivity of the motion sensor, namely that *"the motion sensor is unlikely to respond to a small movement of the unit"*.

47 The ACA recommends that users relying upon this security functionality should conduct their own testing to determine if the sensitivity of the motion sensor is sufficient. However, it should be noted that in its evaluated configuration, the keyed TOE should be kept in a secured environment and operated by trusted personnel (Ref [1]).

48 All other functional tests performed as expected.

3.4 Penetration Testing

49 The developer performed an extensive vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

50 The evaluators also performed an independent vulnerability analysis. The evaluators used the developer vulnerability analysis and their own vulnerability analysis to generate a series of penetration tests. These analyses, and subsequent testing, indicated that the TOE will resist an attacker with a low attack potential.

Chapter 4 - Certification

4.1 Overview

51 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

52 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [20]), the Australasian Certification Authority certifies the evaluation of Datacryptor 2000 performed by the Australasian Information Security Evaluation Facility, LogicaCMG.

53 LogicaCMG has found that Datacryptor 2000 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 4.

54 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

55 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained though an informal model of the TOE security policy.

56 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for obvious vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

57 EAL4 also provides assurance though the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

4.4 Recommendations

58 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ACSI 33 (Ref [2]) and New

Zealand Government users should consult the Government Communications Security Bureau (GCSB).

59 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Refs[1], [3], [4], [5], [6], [7], [8], [9], [10]), the ACA also recommends that users:

a) Determine that the sensitivity of the motion sensor of the TOE is satisfactory before relying upon its security functionality;

b) Wanting to use the SNMP and RIP protocols, configure these protocols securely to ensure that potentially sensitive configuration information is not exposed to the insecure domain.

Annex A - References and Abbreviations

A.1 References

[1] DC2000 Security Target (Common Criteria), Version 1, 0562B218, Thales e-Security Ltd.

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2006, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] DataCryptor 2000 Commercial Version User Manual, 1270A357 Issue 002, Thales e-Security Ltd, June 2003.

[4] DataCryptor 2000 Quick-Start Guide, 1270A363 Issue 001, Thales e-Security Ltd, 2002.

[5] DataCryptor 2000 Release 3.4.1 Release Note (Commercial), 1270A370 Issue 2, Thales e-Security Ltd, 22 July 2003.

[6] DataCryptor 2000 IP, Link, Channelised Link or Frame Relay Network Encryptor – Security Operating Procedures, 1270A461 Issue 001, Thales e-Security Ltd, November 2006.

[7] DataCryptorAP Commercial Version User Manual, 1270A374 Issue 002, Thales e-Security Ltd, July 2004.

[8] Datacryptor AP Quick Start Guide, 1270A378 Issue 001, Thales e-Security Ltd.

[9] DataCryptor AP 100Mbps-IP Release Note AES/3DES 3.511 (Commercial), 1270A391 Issue 7, Thales e-Security Ltd, 26 July 2004.

[10] DataCryptor AP IP Network Encryptor – Security Operating Procedures, 1270A456 Issue 003, Thales e-Security Ltd, December 2006.

[11] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 2003-12-31.

[12] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporate with interpretations as of 14 March 2002.

[13] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporate with interpretations as of 14 March 2002.

[14] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 14 March 2002.

[15] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[16] AISEP Publication No. 2 – Certifier Guidance, AP 2, Version 3.0, 21 February 2006, Defence Signals Directorate.

[17] AISEP Publication No. 3 – Evaluator Guidance, AP 3, Version 3.1, 29 September 2006, Defence Signals Directorate.

[18] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4, Version 3.1, 29 September 2006, Defence Signals Directorate.

[19] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[20] Thales Datacryptor 2000 and Datacryptor Advanced Performance Evaluation Technical Report, Issue 1.0, 30 April 2007, LogicaCMG.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DC2K	Datacryptor 2000
DCAP	Datacryptor Advanced Performance
DEK	Data Encryption Key
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
PP	Protection Profile
RoHS	Restriction of the use of certain hazardous substances in electrical and electronic equipment
SFP	Security Function Policy
SFR	Security Functional Requirements
SGSS	Secure Generic Sub-System
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy