RED ALERT LABS
IoT Security

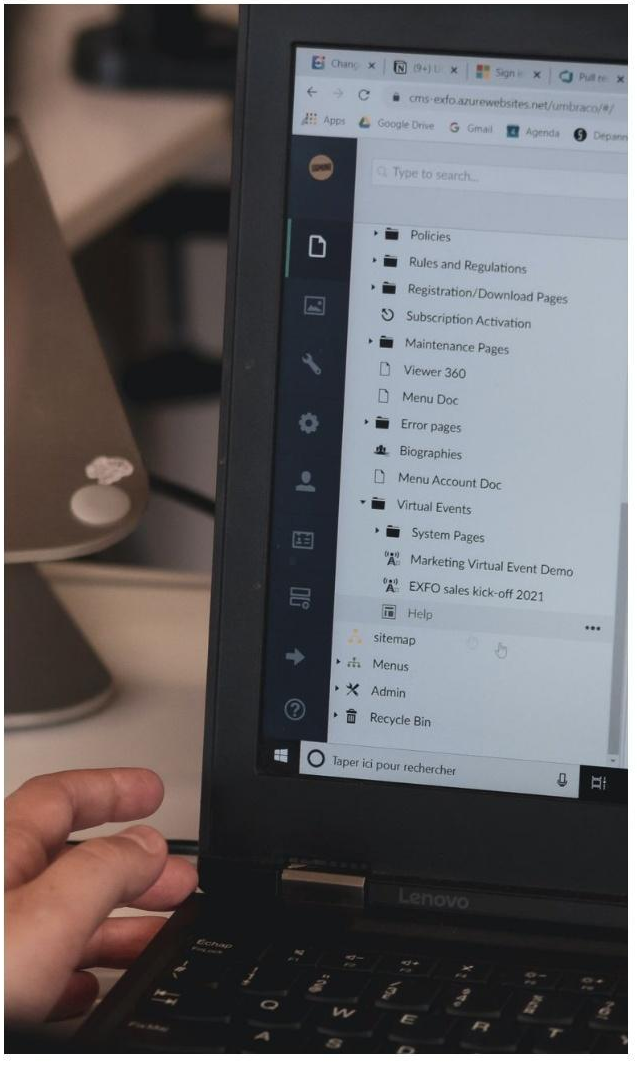
TRUSTBOOST

CC Training Use Case Study

17/06/2025

TrueCrypt Samples

Creation of Evidence Documentation



Security Target

ITR ASE

SECURITY TARGET

TOE Identification & Declaration of Conformity

Extract of the certified **TrueCrypt** software document.
ST & ToE Reference + Declaration of conformity.

1.1 Identification of the security target (ST)

Title :	TRUECRYPT security target
Version :	2.0
Author	Silicomp-AQL
Reference :	SPM030-ST-2.0
Date of publication :	October 22, 2007

1.2 Identification of the target of evaluation (TOE)

Developer name:	TrueCrypt Foundation
Product name:	TRUECRYPT
Product version:	4.2a
TOE perimeter:	The TOE perimeter is limited to the following cryptographic algorithms: AES-256, TWOFISH, AES-TWOFISH, SHA1 and RIPE-MD 160 (see §1.4.2)
Target platforms:	PC platforms under Microsoft Windows XP (see §1.4.2)

2 Declaration of conformity

2.1 Common Conformity Criteria

This security target conforms to parts 2 and 3 of version 3.1 of the Common Criteria ([CC2] and [CC3]).

2.2 Conformity to a protection profile

This security target does not conform to any identity protection profile[4].

2.3 Conformity to an insurance packet

The level of evaluation assurance aimed for by this security target is EAL2+ (or augmented EAL2), augmented by the following components :

- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- ALC_TAT.1
- AVA_VAN.3.

SPD

SECURITY TARGET

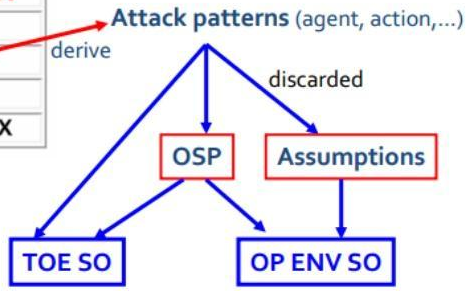
- Security Problem Definition

ATTACK PATTERNS (AGENT, ACTION,…) DERIVE TOE SO & OP ENV SO

DISCARDED ASSUMPTIONS OSP

MANY APPROACHES: RISK/THREAT ANALYSIS, THREAT DB, …., A SIMPLE ONE

ASSETS / IMPACT	C	I	A
A1	X		
A2	X	X	
.....			
An		X	X



© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Security Functionalities in the ST

SF.MASTER_KEY_GEN	This security function enables the generation of the master key associated with a disk.
SF.CIPHERING	This security function enables the writing of ciphered data on a previously mounted 'ciphered disk' using ciphering keys and algorithms associated with this 'ciphered disk'.
SF.DECIPHERING	This security function enables the reading of ciphered data on a previously mounted 'ciphered disk' using ciphering keys and algorithms associated with this 'ciphered disk'.
SF.HASH_CALC	This security function ensures the hash calculation of data associated with a 'ciphered disk', according to the hash calculation algorithm associated with this 'ciphered disk'.
SF.CLEANNING	This security function makes it possible to delete sensitive data which could temporarily be found in unprotected zones. For example, the password contained in the RAM may turn up in the SWAP zone of the operating system.

©2025 Proprietary and Confidential. All Rights Reserved.

Assets & Threats

TSF Data	D.DONNEES_AUTH	This asset represents authentication data which is used to verify the identity given by a user (user password and possibly keyfiles)
TSF Data	D.CLE_ENTETE	This asset represents the header key used to cipher header data containing, particularly, the master key. This key is obtained by derivation from data authentication.
TSF Data	D.CLE_MAITRE	This asset represents the master key used to cipher the users' data.
User Data	D.DONNEES_UTILISATEUR	This asset represents the user data to be protected confidentially on the disk by the TOE. It is unscrambled data (ciphered data is not sensitive asset).
Threat	T.ACCES_DONNEES	A hacker discovers the user's sensitive data which is stored on the disk - for example, after getting hold of one or several partial or complete disk image(s) (possibly at different times) or after stealing the equipment or the disk.

©2025 Proprietary and Confidential. All Rights Reserved.

Organisational Security Policies & Assumptions

OSP	OSP.CRYPTO	The TOE's cryptographic mechanisms must conform to the requirements of the DCSSI's cryptographic frame of reference concerning standard robustness level.
Hypothesis	A.ENV_OPERATIONNEL	The operational environment does not allow a hacker to access the disk when sensitive data is accessible to a legitimate user of the equipment.

©2025 Proprietary and Confidential. All Rights Reserved.

Security Objectives

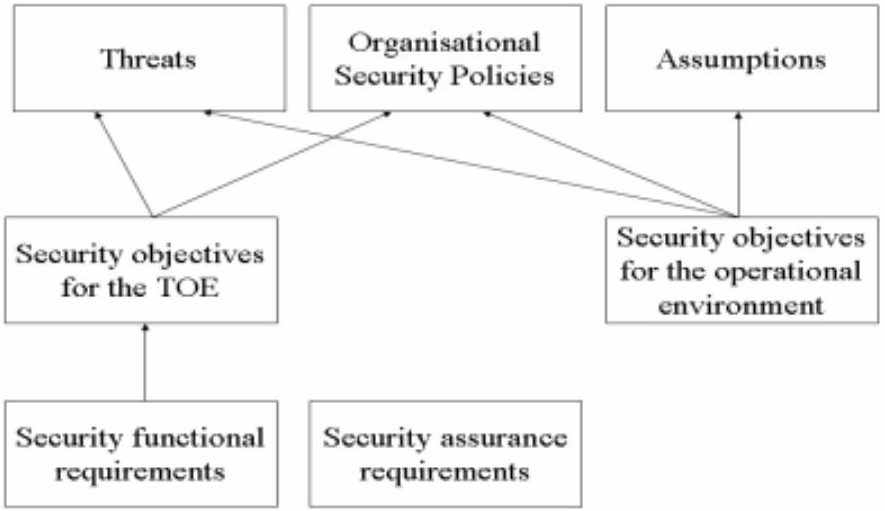
ToE SO	O.CRYPTO	The TOE must implement cryptographic functions and handle cryptographic keys in conformity with the requirements of the DCSSI's cryptographic frame of reference concerning standard robustness level.
ToE SO	O.PROTECTION_DES_DONNEES_ENREGISTREES	The TOE must ensure that the user has been authenticated before making recorded data accessible.
ToE SO	O.CLES_CHIFFREMENT	The TOE must generate ciphering keys (master keys) which can ensure the confidentiality of the user's sensitive data.

Op. env. SO	OE.ENV_OPERATIONNEL.1	When the user has been authenticated, the operational environment must ensure the confidentiality of sensitive data, authentication keys and data.
Op. env. SO	OE.ENV_OPERATIONNEL.2	The user must access his sensitive data only when he is in a trustworthy environment (when he is alone or with people who need to be familiar with it).

©2025 Proprietary and Confidential. All Rights Reserved.

Security Objectives Coverage

SECURITY TARGET



If all SFRs and SARs are satisfied and all SOs for the operational environment are achieved, **then** the security problem is solved.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Security Functional Requirements(SFR) & Coverage

FCS_CKM	Cryptographic key management	.1 --> Cryptographic key generation .3 --> Cryptographic key access .4 --> Cryptographic key destruction
FCS_COP	Cryptographic operation	.1 --> Cryptographic operation
FMT_MTD	Management of TSF data	.1 --> Management of TSF data .2 --> Management of limits on TSF data .3 --> Secure TSF data

ToE SO	O.CRYPTO	FCS_CKM.1, FCS_CKM.3, FCS_CKM.4, FCS_COP.1, FMT_MTD.3
ToE SO	O.CLES_CHIFFREMENT	FCS_CKM.1, FMT_MTD.3

©2025 Proprietary and Confidential. All Rights Reserved.

SFRs mapping to SFs

SF.MASTER_KEY_GEN	FCS_CKM.1, FMT_MTD.3
SF.CIPHERING	FCS_COP.1
SF.DECIPHERING	FCS_COP.1
SF.HASH_CALC	FCS_CKM.1, FCS_COP.1
SF.CLEANNING	FCS_CKM.4, FDP_RIP.1

©2025 Proprietary and Confidential. All Rights Reserved.

SAR provided by the vendor for Truecrypt

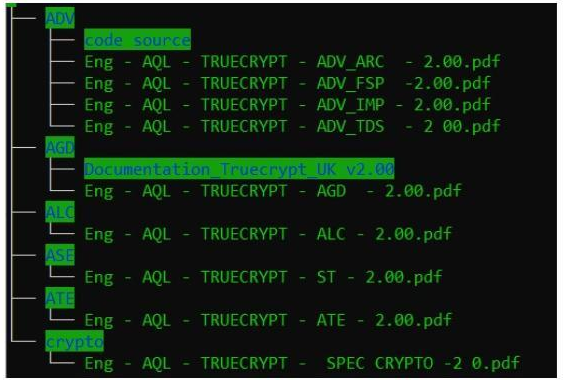
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Extract from the ST:

2.3 Conformity to an insurance packet

The level of evaluation assurance aimed for by this security target is EAL2+ (or augmented EAL2), augmented by the following components :

- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- ALC_TAT.1
- AVA_VAN.3.



SAR provided by the vendor

SARs & EAL

	Evaluation Assurance Level	EAL 2+ (augmented)
SUBSTANTIAL	SAR package	AGD_PRE.1 ALC_CMC.2 ALC_CMS.2 ALC_DEL.1 ASE_CCL.1 ASE_ECD.1 ASE_REQ.2 ASE_ECD.1 ASE_INT.1 ASE_OBJ.2 ASE_REQ.2 ASE_SPD.1 ASE_TSS.1
HIGH	Augmented SARs (due to a whitebox evaluation)	☒ ADV_FSP.4 ☒ ADV_TDS.3 ☒ ADV_IMP.1 ☒ ALC_TAT.1 ☒ AVA_VAN.3.

©2025 Proprietary and Confidential. All Rights Reserved.

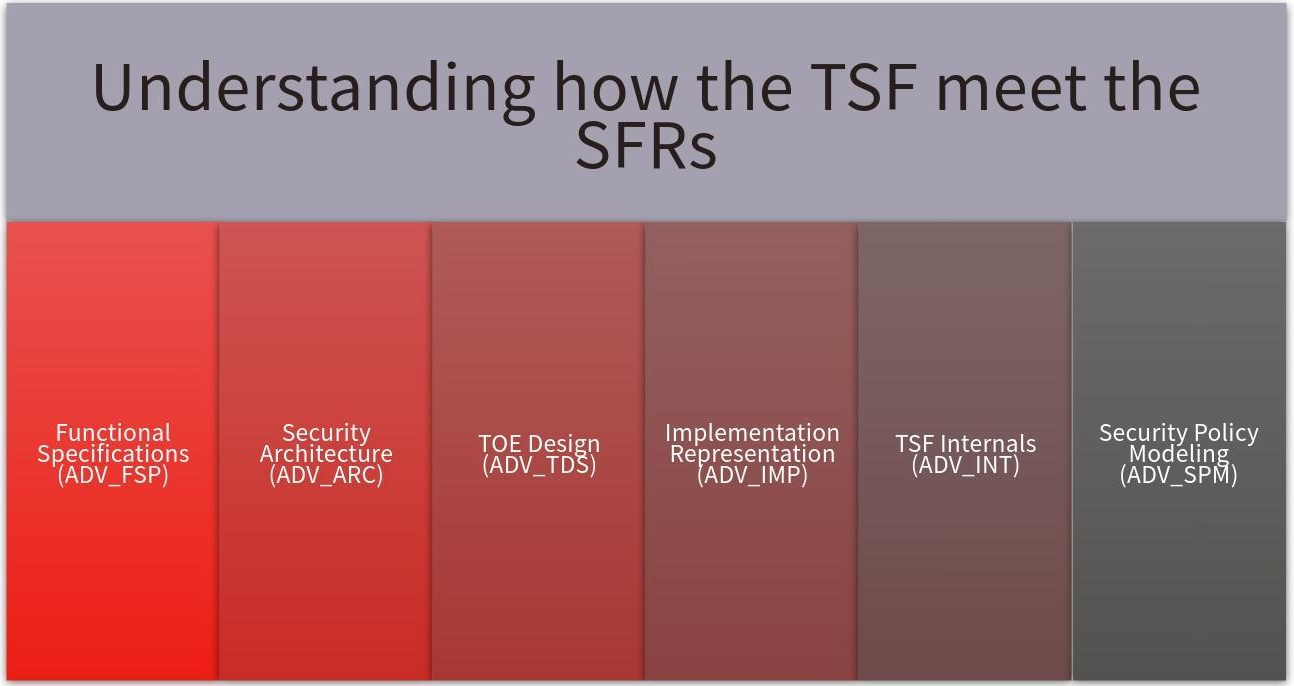
RED ALERT LABS
IoT Security

Development Evidence

ITR ADV

SAR
DEVELOPMENT (ADV)

Verify the vendor's security functional claims



© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

PHASE 2: CONDUCT - SAR
FUNCTIONAL SPECIFICATION (ADV_FSP)

Describe the TSFI

- Purpose
- Method of use
- Parameters
- Actions
- Error messages

Mapping with the SFR

(EAL 5) The functional specification shall describe the TSFI using a semi-formal style.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt TSFI

ADV_FSP.4

This is an extract from the ADV_FSP documentation provided by the vendor for **Truecrypt**.

This part present the means provided to users to access different TrueCrypt services.
The following table highlights links between services and services access interfaces.
The third column identifies interfaces to take into account within the framework of the evaluation (TSFI).

Servicies	Services access interfaces	TSFI
Creation of a ciphered disk	Creating a ciphered disk (§4.4)	X
Creation of a hidden ciphered disk		
Creation of a traveling ciphered disk (autonomous volume which functions without having to install TrueCrypt)	Creating a traveling disk (§4.18)	
On-the-fly ciphered volume ciphering / deciphering	Writing on a ciphered disk (§4.7)	X
	Reading on a ciphered disk (§4.8)	X
Generation of keyfiles	Generating a keyfile (§4.11)	X
Ciphering algorithm performance tests	Carring out performance and cryptographic mechanism conformity test (§4.17)	
Ciphering algorithm conformity tests		
Backup volume headers	Backup volume headers (§4.19)	
Restore volume headers	Restore volume headers (§4.20)	
Configuration of the software via the 'preferences' menu	Changing TrueCrypt configuration (§4.16)	
Changing a ciphered disk's protection means	Modifying a ciphered disk's password (§4.9)	X
	Adding / deleting a keyfile to/from a ciphered disk (§4.10)	X
	Modifying the hash algorithm of a ciphered disk (impact on the generation of header keys) (§4.12)	X
Management of the application	Starting TrueCrypt (§4.2)	X
	Exiting TrueCrypt (§4.3)	X
Management of the ciphered disk access	Mounting a disk (§4.5)	X
	Dismounting a disk (§4.6)	X
	Wipe cached password (§4.13)	X
Information display	Displaying mounted ciphered disk information (§4.14)	

Truecrypt TSFI description sample

ADV_FSP.4

This is an extract from the ADV_FSP documentation provided by the vendor for **Truecrypt**.

4.2.1 *Functioning*

Starting TrueCrypt	
This function is carried out when TrueCrypt.exe is run. This results in the running of the TrueCrypt.exe executable. The application starts by loading the TrueCrypt driver or by attaching itself to it (if it is already loaded). In the event of failure, the application can not initialise properly and closes down. Once the driver is loaded (or attached), TrueCrypt runs its interface and listes the volumes already mounted (if the driver was already in memory before it started up).	
Input interfaces	**Input data**
Windows HMI	TrueCrypt stopped
Method of use	
Double click on the "TrueCrypt.exe" or on one of this shortcut OR Auto-start upon log on to Windows (check box in the "Preferences" window).	
Actions	
Load TrueCrypt driver *Locking sensitive global variables in memory* **Initialisation** Running interface	
Output interfaces	**Output data**
TrueCrypt HMI	TrueCrypt started
SFR	
FDP_RIP.1 Subset residual information protection FMT_MSA.3 Static attribute initialisation	

Truecrypt TSFI x SFR

ADV_FSP.4

This is an extract from the ADV_FSP documentation provided by the vendor for **Truecrypt**.

TSFI	Actions	FCS_CKM.1/ Header key	FCS_CKM.1/ Master key	FCS_CKM.3/ header_key	FCS_CKM.3/ master_key	FCS_CKM.4	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FDP_RIP.1	FIA_UID.1/ disk owner	FIA_UAU.1/ disk owner	FIA_SOS.1/ password	FMT_MOF.1/ disk owner	FMT_MSA.2	FMT_MSA.3	FMT_MTD.1/ auth_data	FMT_MTD.1/ master_key	FMT_MTD.1/ header_key	FMT_MTD.2/ auth_data	FMT_MTD.3	FMT_SMF.1	FMT_SMR.1	FPT_FLS.1	FRU_FLT.1
Creating a ciphered disk	Generation of header keys from the seed and modified password	X					X							X					X		X				
	Generation of master keys		X				X							X	X			X			X				
	Creation of ciphered disk's header (contains the master keys and seed)				X		X								X										
	Ciphering header with header keys (exept the seed)			X		X	X								X										
	Writing ciphered disk's header.							O	O						X										
	Formating ciphered disk						X	O	O												O				
Mounting a disk	Generation of modified password from user password and keyfiles						X	X	X		X	X									X	X			
	Generation of header keys from the seed and modified password	X					X	X	X		X	X							X		X				
	Deciphering ciphered disk's header using header keys			X			X																X		
	Extraction of master keys from the deciphered header				X	X												X							
Writing onto a disk	Request to TrueCrypt driver to write onto mounted ciphered disk				X		X	X	X																
Reading on a disk	Request to TrueCrypt driver to read on mounted ciphered disk				X		X	X	X																

PHASE 2: CONDUCT - SAR
TOE DESIGN (ADV_TDS.3)

- Describe the TSF boundary
- How the TSF implement the SFRs ?
- Definition of Subsystems and Modules + mapping with the TSFI
    - SFR-enforcing
    - SFR-supporting
    - SFR-non-interfering

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt - TOE Design

ADV_TDS.3

This is an extract from the ADV_TDS documentation provided by the vendor for **Truecrypt**.

4.2 Description of TSF modules

1. Application management subsystem			
Start-up	Function	This module is launched when TrueCrypt.exe is executed. This results in the launching of the TrueCrypt.exe executable The application begins by loading the TrueCrypt driver (or by attaching itself to it if it is already loaded). In the event of failure, the application cannot initialise correctly and closes down. Once the driver is loaded (or attached), TrueCrypt locks the sensitive glbal variables into memory (using the Windows *VirtualLock* function). Finally, the application launches the user interface and the list of volumes already mounted (if the driver was already in the memory before start-up).	
	Interface(s) presented / Return value(s)	WINMAIN	0
	Interactions	N / A	
Settings	Function	This module enables TrueCrypt settings to be changed Configuration concerns : - default mounting options, - functioning of TrueCrypt as a fundamental task, - actions carried out when Windows starts up or when a session opens, - automatic dismounting conditions, - TrueCrypt interactions with Windows, - password chache policy.	
	Interface(s) presented / Return value(s)	PreferencesDlgProc	0
	Interactions	N / A	

PHASE 2: CONDUCT - SAR
IMPLEMENTATION REPRESENTATION (ADV_IMP.1)

Mapping between the implementation representation (source code) and the TOE design of the TSF.

Determine if the implementation is sufficient enough to satisfy the Security Requirements of the Security Target

Describe the TSF implementation

Understand implementation details for Vulnerability analysis

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt - IMPLEMENTATION REPRESENTATION

ADV_IMP.1

This is an extract from the ADV_IMP documentation provided by the vendor for **Truecrypt**.

Sub-system name	Module name	Corresponding C File	Corresponding function
Application management			
	Start TrueCrypt	Mount.c	WINMAIN
	Set TrueCrypt parameters	Mount.c	PreferencesDlgProc
	Tests	Benchmark Dlgcode.c	PerformBenchmark
		Test des vecteurs Dlgcode.c Test.c	CipherTestDialogProc AutoTestAlgorithms
	Close TrueCrypt	Mount.c	localcleanup

PHASE 2: CONDUCT - SAR
SECURITY ARCHITECTURE (ADV_ARC)

- Description of Security Domains
- Description of Initialization process
- Self protection
- Prevent bypassing of TSF
- Support the claims of the TSF.
- Consistency with the TOE design (ADV_TDS)

→ **ALL THE MODULES MUST BE FOUND IN BOTH DOCUMENTS.**

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt - ADV_ARC.1

Security Architecture

This is an extract from the ADV_ARC documentation provided by the vendor for **Truecrypt**.

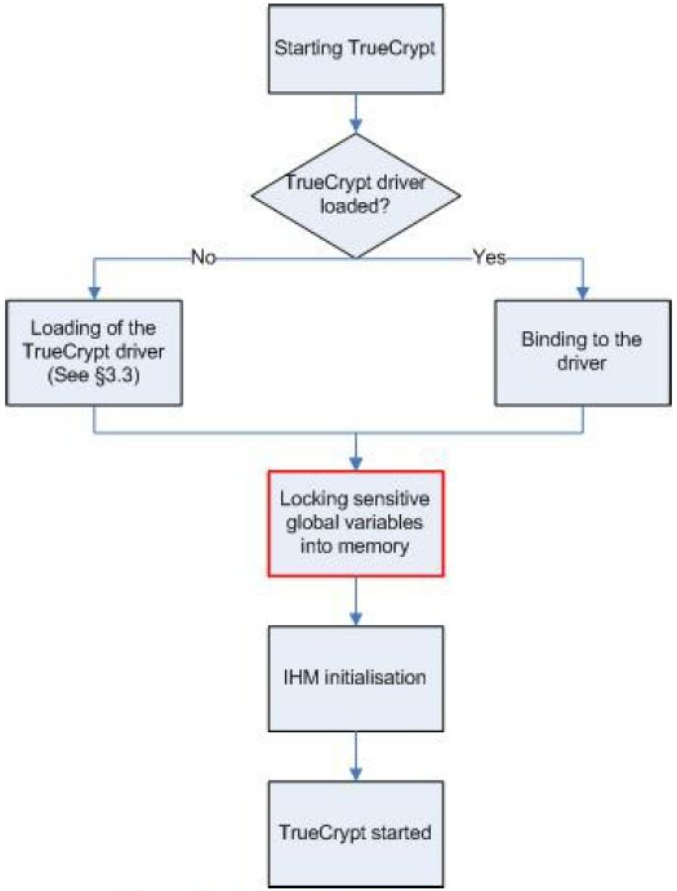


Figure 2 - TrueCrypt.exe start-up process

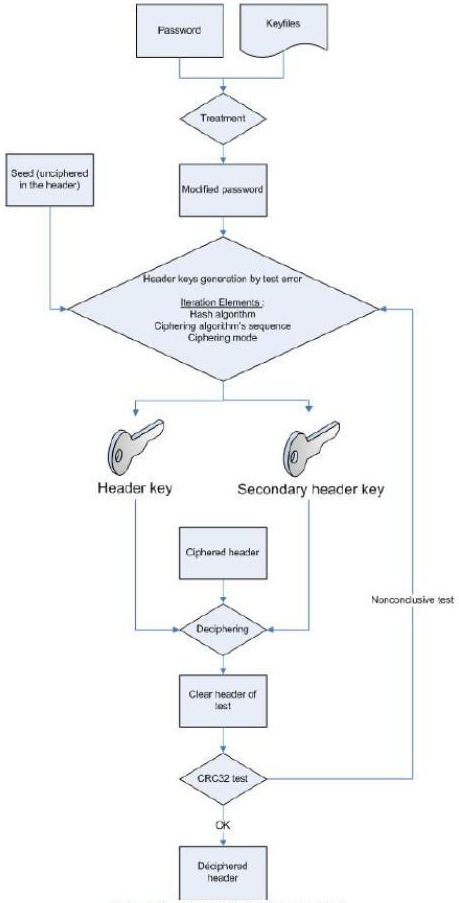
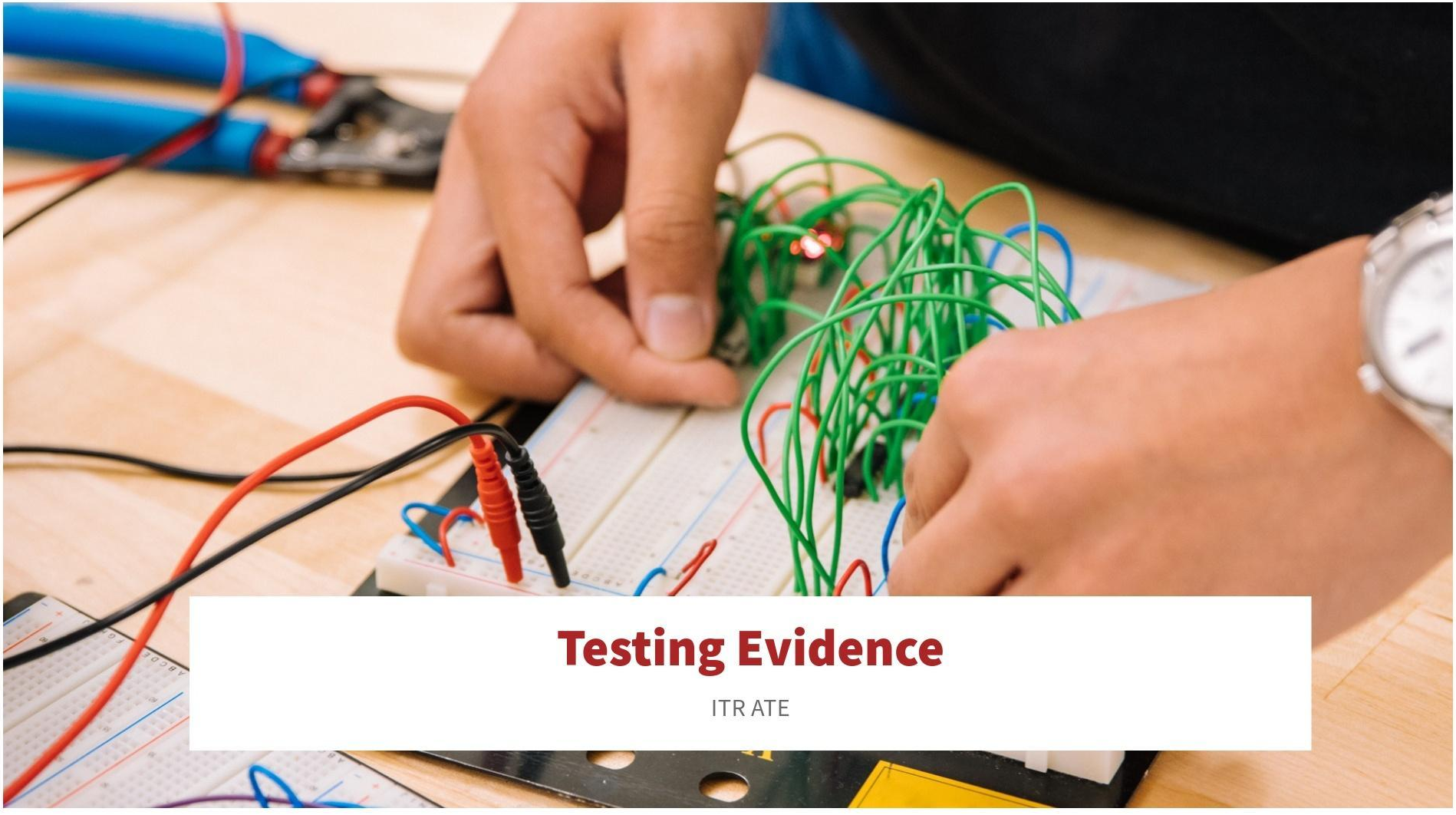


Figure 5 – Header deciphering process



Testing Evidence

ITR ATE

PHASE 2: CONDUCT - SAR
TEST EVIDENCE (ATE)

- **Confirm that the TOE security functionalities perform as designed.**

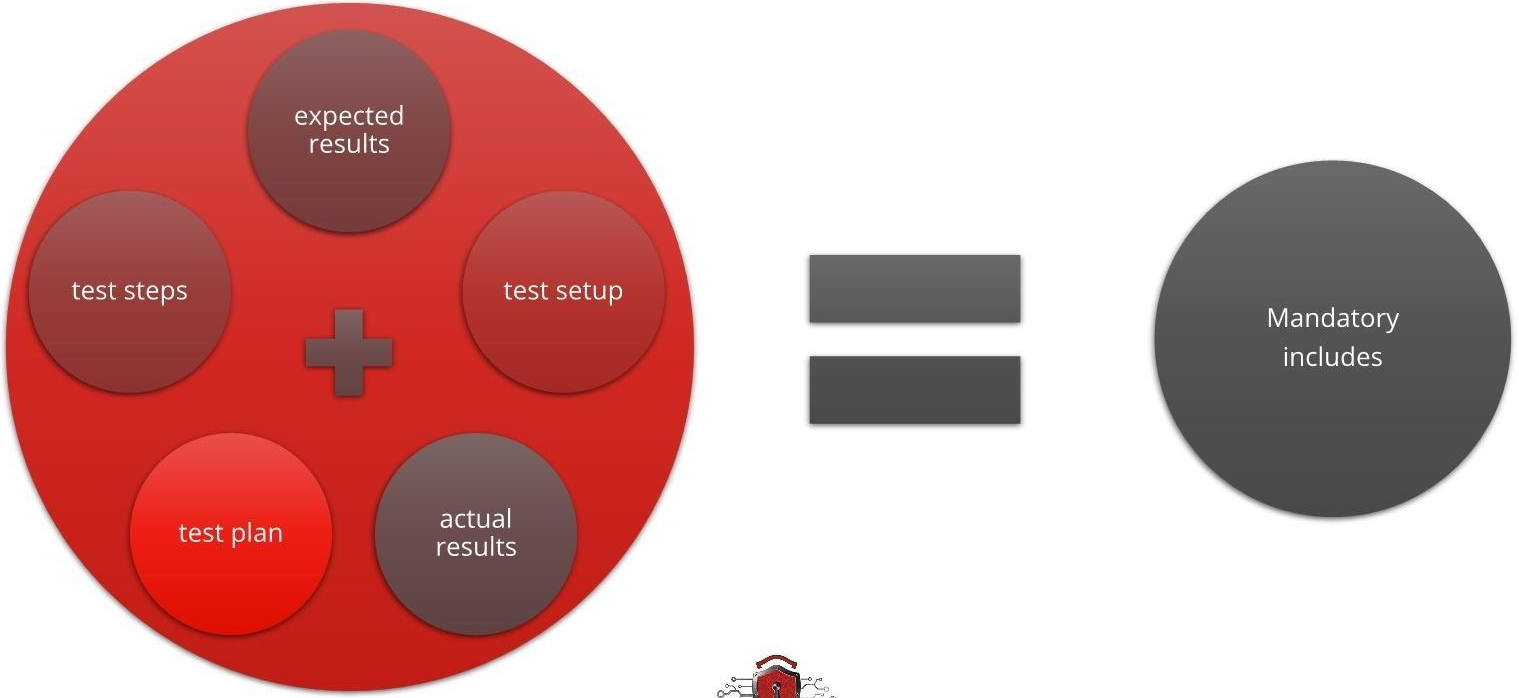
Correlate to the functional specification & the Security Target

Close involvement of the QA team members.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

PHASE 2: CONDUCT - SAR
FUNCTIONAL TESTS (ATE_FUN)

- Describes the tests performed by the developer on security functionalities claimed in the ST.



© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt - ATE_FUN.1

Functional Testing

This is an extract from the ATE documentation provided by the vendor for **Truecrypt**.

3.1.1 Tests CREATE_01

3.1.1.1 Aim of the test

This test aims at checking that a user with non-root privileges can create a ciphered disk in a container file, using a key file. The file system on the encrypted disk is FAT.

3.1.1.2 Prerequisites

- The TrueCrypt driver must be loaded in memory.
  - The user can set TrueCrypt to start automatically on boot, and reboot its computer.
  - OR the root user runs TrueCrypt.

3.1.1.3 Procedure

- Launch the « Create volume » wizard:
  - The user executes « TrueCrypt Format.exe »
  - OU the user executes « TrueCrypt.exe » and click on « Create Volume »
- The user clicks on the « Next » button
- The user selects the path of the container file by clicking on « Select File »
- The user clicks on the « Next » button
- The user selects the hash and crypt algorithms
- The user clicks on the « Next » button
- The user types a file size of 20Mo
- The user clicks on the « Next » button
- The user types his 15 characters long password in the « Password » and « Confirm » fields
- The user checks the box « Use keyfiles »
- The user clicks on the « Keyfiles » button
- The user clicks on the « Generate Random Keyfile… » button
- The user clicks on the « Generate and Save Keyfile » and types the path of his key file
- The user closes the random generation window by clicking on the « Close » button
- The user clicks on the « Add File » button
- The user clicks on the « OK » button
- The user clicks on the « Next » button
- The user selects the FAT file system
- The user clicks on the « Format » button

3.1.1.4 Expected results

TrueCrypt says the encrypted disk was created successfully.

Truecrypt - Samples
TEST COVERAGE (ATE_COV.1)

Describes the breadth of test coverage performed by developers across the TOE module interfaces.

(ATE_COV.1)

demonstrate that all the TSFI has been tested

mapping table between SFR, TSFI and tests details

	Relevance	Coverage	CREATE_01	CREATE_02	CREATE_03	CREATE_EXCEP_01	CREATE_EXCEP_02	CREATE_EXCEP_03	CREATE_EXCEP_04	MOUNT_01	MOUNT_02
Display information about a mounted encrypted disk	0	-1									
Display the drives corresponding to the mounted disks	0	-1								1	1
Add / remove a keyfile of a ciphered disk	1	3									
Change TrueCrypt settings	0	-1									
Create a ciphered disk	1	7	1	1	1	1	1	1	1		
Create a traveller disk	0	-1									
Start TrueCrypt	0	-1									
Dismount a disk	1	1									
Write on a ciphered disk	1	1									
Perform benchmarks and conformity tests on the crypting routine	0	-1									
Create a keyfile	1	1									
Read from a ciphered disk	1	1									
Change the hash algorithm of a ciphered disk	1	3									
Change the password of a ciphered disk	1	3									
Mount a disk	1	3								1	1
Exit TrueCrypt	1	1									
Wipe cache password	1	2									
Backup volume header	1	1									
Restore volume header	1	1									

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

INDEPENDENT TESTS (ATE_IND)

Intended to provide greater assurance over developer testing.

(ATE_IND)

Developed by the evaluator.

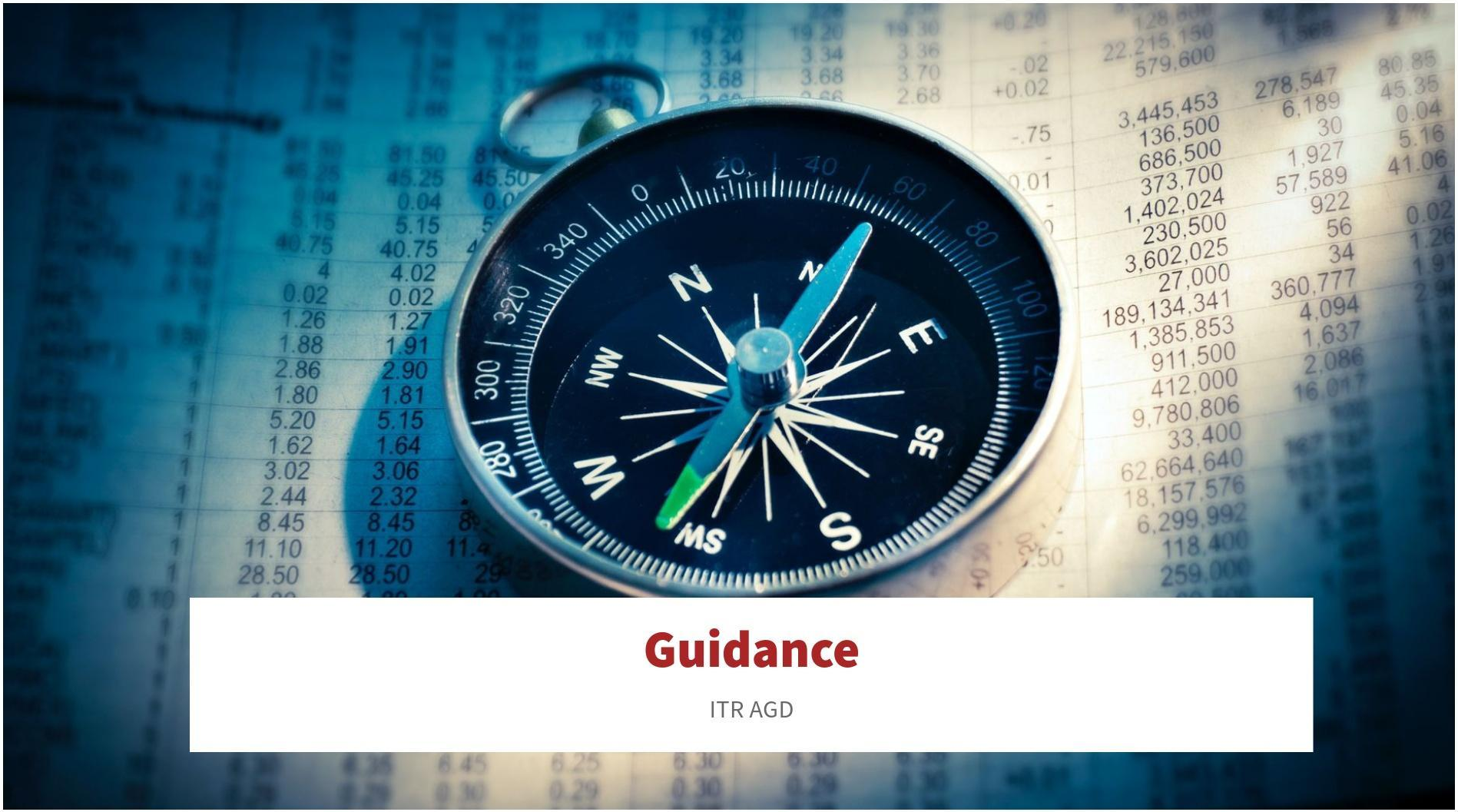
Requires the developer to provide the TOE and an equivalent test environment so that the evaluator so the evaluator can run a subset of the developer's tests.

COULD NEGOTIATE THIS TO HAPPEN DURING THE EVALUATOR'S ON-SITE VISIT

A.1 Analysis of developer tests

Function Tested	Test Identifier	Results obtained by the developer	Results obtained by the evaluator	Conformity with developer tests
Create a ciphered disk	CREATE_01	TrueCrypt indicates that the ciphered disk has been successfully created.	Message confirming creation of ciphered disk.	Conforms
	CREATE_02	TrueCrypt indicates that the ciphered disk has been successfully created.	Message confirming creation of ciphered disk.	Conforms
	CREATE_03	TrueCrypt indicates that the hidden ciphered disk has been successfully created	Message confirming creation of hidden ciphered disk	Conforms
	CREATE_EXCEP_01	A window appears, indicating that the password is too short. TrueCrypt asks the user if he wishes to continue or change his password.	Warning that the password is too short. TrueCrypt gives the option to continue all the same, or to change the password.	Conforms
	CREATE_EXCEP_02	The 3 first password entries must be accepted. The fourth entry generates an error message that reminds the user which characters are authorised.	Only ASCII characters are authorised.	Conforms

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED



Guidance

ITR AGD

PHASE 2: CONDUCT - SAR
PREPARATIVE GUIDANCE (AGD_PRE)

Provides information to the users on how to securely install and configure the TOE

include directions on securing the operational environment.

must be consistent with the ALC_DEL.

minimum system requirements

requirements of the operational environment

...

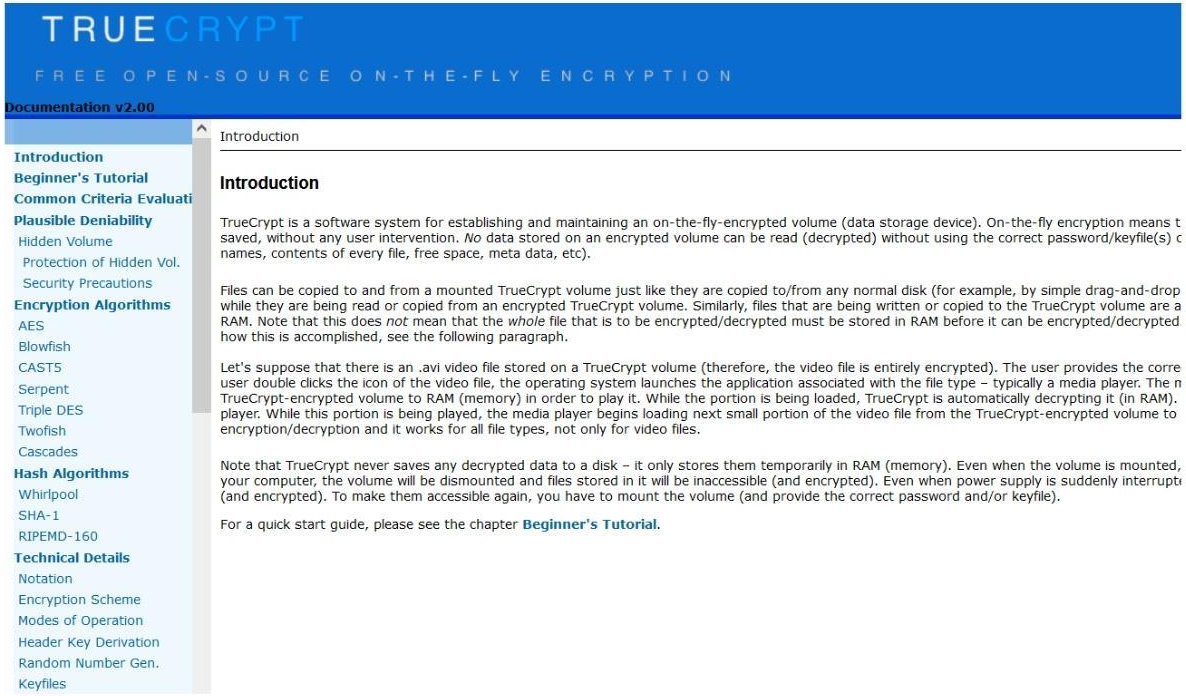
© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt - Samples
OPERATIONAL GUIDANCE (AGD_OPE)

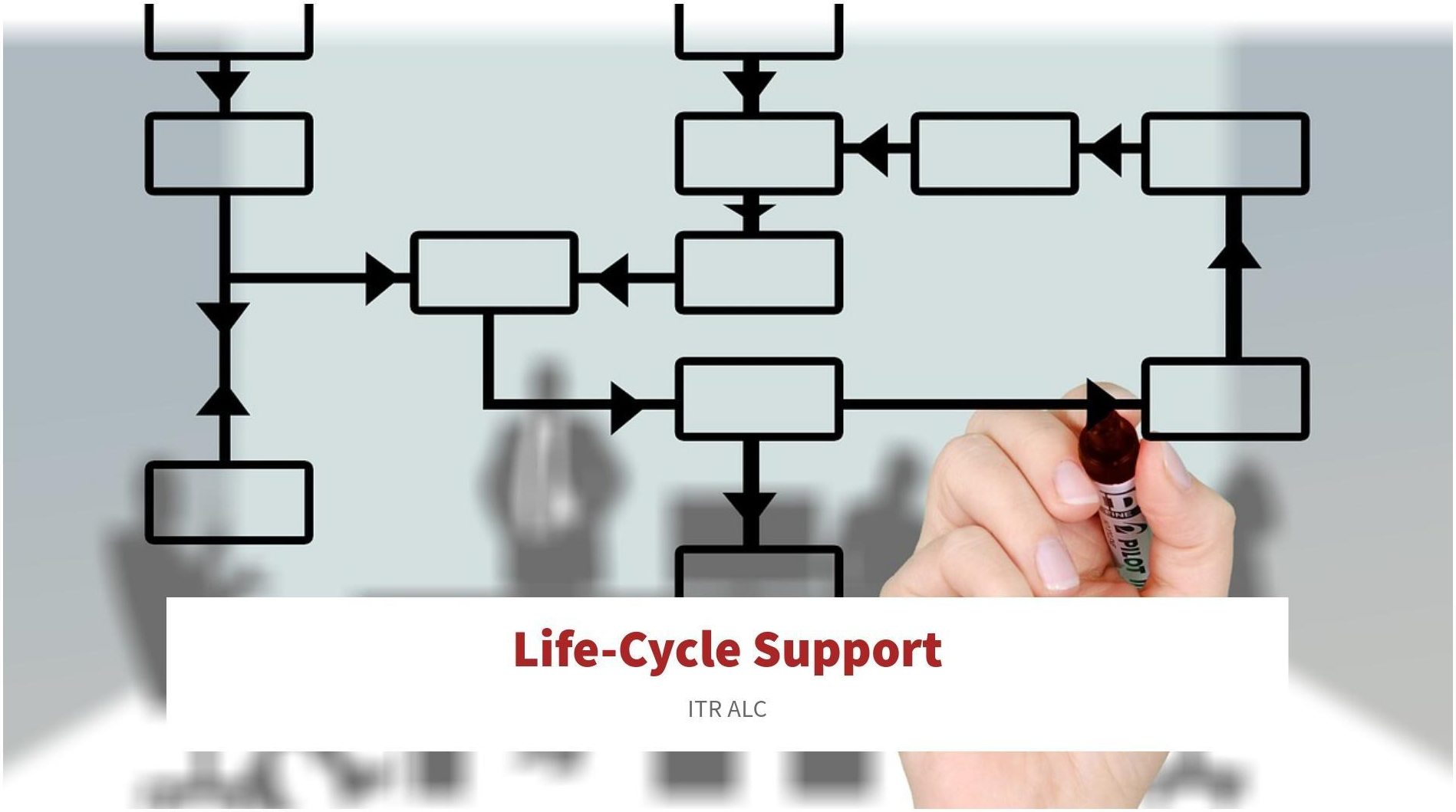
Describes to the user the security functionality of the TOE

(AGD_OPE)

- role specific functions and privileges
- methods available to the user
- authorized parameters
- responses or error codes



© 2020 RED ALERT LABS – ALL RIGHTS RESERVED



Life-Cycle Support

ITR ALC

Life-Cycle - Truecrypt - Samples
TOOLS & TECHINQUES (ALC_TAT.1)

Describes the developer's use of tools.

- compilers
- testing tools
- …

It includes requirements to prevent ill-defined, inconsistent or incorrect development tools from being used to develop the TOE.

3 Development tools

This chapter answer to the component ALC_TAT.1 relating to the tools used during the development.
Following information is present in the text file "Readme.txt" delivered with the file containing the source code.

3.1 Tools identification

Development language :	C
Development environment:	Microsoft Visual Studio .NET 2003 (version 7.1) or compatible
Additional component :	Windows 2003 SP1 Driver Development Kit (build 3790.1830) or compatible

The archive contain a file « TrueCrypt.sln » corresponding to a Visual Studio solution.
This solution is composed of this five following projects:

- Crypto
- Driver
- Format
- Mount
- Setup

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt - Samples

CONFIGURATION MANAGEMENT SCOPE (ALC_CMS)

- What is managed by the configuration system ?
  - e.g the source code, documentation, tools, etc.
- Problem tracking (security flaw reports) shall be covered

2.1 TrueCrypt 4.2a source code

Source code versions are managed by a CM system making it possible to have a single identifier for each configuration item.

The source code is composed of the following files:

Folder	Header files	C files
Common	GfMul.h Format.h Keyfiles.h Fat.h Language.h Apidrvr.h Endian.h Dlgcode.h Dictionary.h Password.h Crypto.h Pkcs5.h Crc.h Progress.h Xml.h Random.h Common.h Registry.h Resource.h Tcdefs.h Combo.h Cmdline.h Tests.h Volumes.h Cache.h	Tests.c Combo.c Xml.c Registry.c Cmdline.c Volumes.c Crc.c Progress.c Crypto.c Pkcs5.c Dictionary.c Password.c Dlgcode.c Cache.c Endian.c Random.c Fat.c Language.c Format.c Keyfiles.c GfMul.c
Crypto	Serpent.h Des.h Cast_s.h Des_locl.h Cast_lcl.h	Aescrypt.c Aeskey.c Twofish.c Aestab.c Whirlpool.c

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

PHASE 2: CONDUCT - SAR
CONFIGURATION MANAGEMENT CAPABILITIES (ALC_CMC)

- Ensure that the TOE is correct and complete before it is sent to the customer
- Ensure that no configuration items are missing during evaluation
- Prevent unauthorized modification, addition or deletion of TOE configuration items

Roles, responsibilities, procedures, bug tracking, access control, etc.

→ on-site visit from the evaluator is required

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Truecrypt - Samples

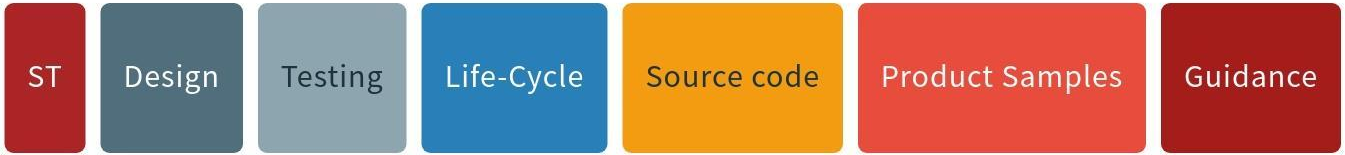
DELIVERY PROCEDURES (ALC_DEL.1)

ALC_DEL.1.1C	**The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.**		
	ALC_DEL.1-1	The evaluator shall examine the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.	Each archive is signed with PGP under an unconnected system. Then, the archive is uploading on the truecrypt.org server with WinSCP (SSL connexion). On the user side, its possible to verify, with the public PGP key, the originality and the integrity of the TOE downloaded.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Evidence Delivery

To Send to the ITSEF



©2025 Proprietary and Confidential. All Rights Reserved.

RED ALERT LABS
IoT Security

#3 Evaluation Process

ITSEF

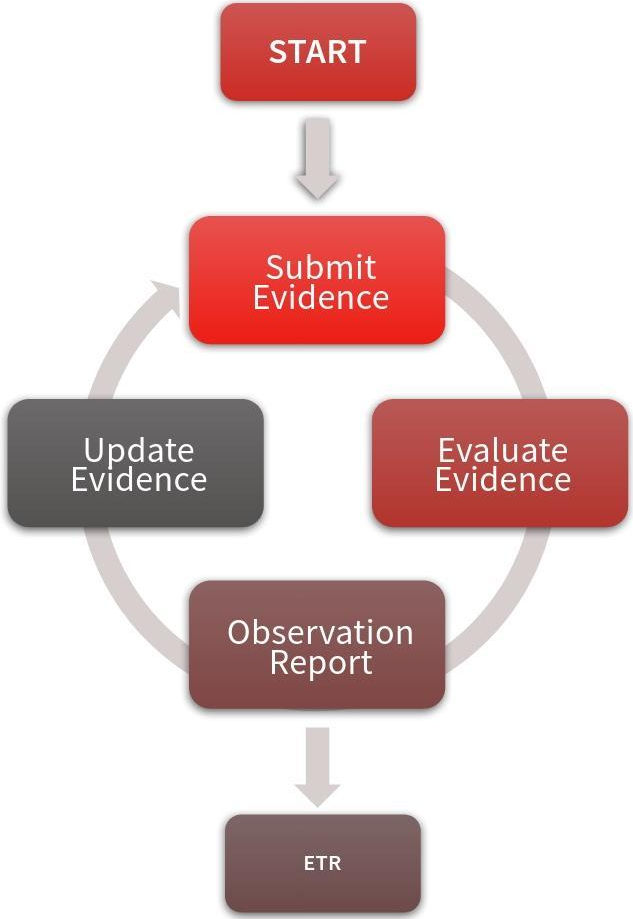
EVALUATION PROCESS
CC Evaluation Methodology

- If the evaluator find an inconsistency or some missing information or error in the evidence documentation

 produces an OR

Will not give much information on how to rectify the situation (depends on the lab)

Avoid evaluators who provide ambiguous feedback such as FSP are inconsistent with ST



© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Evaluation Approach

1. Thorough reading of the elements using information from technical control sheets;
2. Pooling of technical control sheets during an informal review;
3. Where appropriate, conduct independent traceability analysis;
4. Comparison with Common Criteria evaluation requirements;
5. Establishing verdicts;
6. Drawing up of the current Technical Evaluation Report for the corresponding component
7. Verification of report by the ITSEF technical manager.

©2025 Proprietary and Confidential. All Rights Reserved.

RED ALERT LABS
IoT Security

Evaluation activities in scope for **Truecrypt**

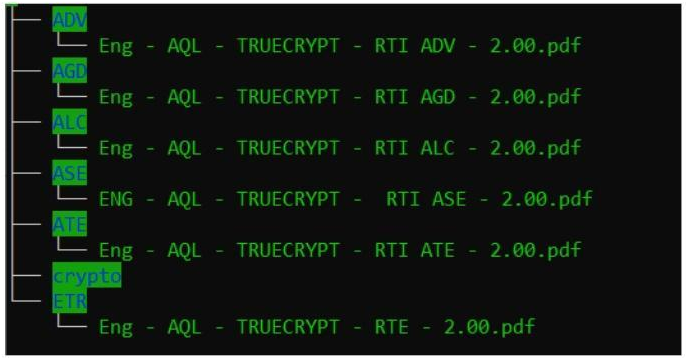
Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Extract from the ST:

2.3 Conformity to an insurance packet

The level of evaluation assurance aimed for by this security target is EAL2+ (or augmented EAL2), augmented by the following components :

- ADV_FSP.4
- ADV_TDS.3
- ADV_IMP.1
- ALC_TAT.1
- AVA_VAN.3.



Reports produced by the ITSEF

PHASE 3: RECOVER & FINALIZE
EVALUATION TECHNICAL REPORT (ETR)

- CC evaluation labs are required to produce and send reports to the national scheme
- These reports are called ETRs

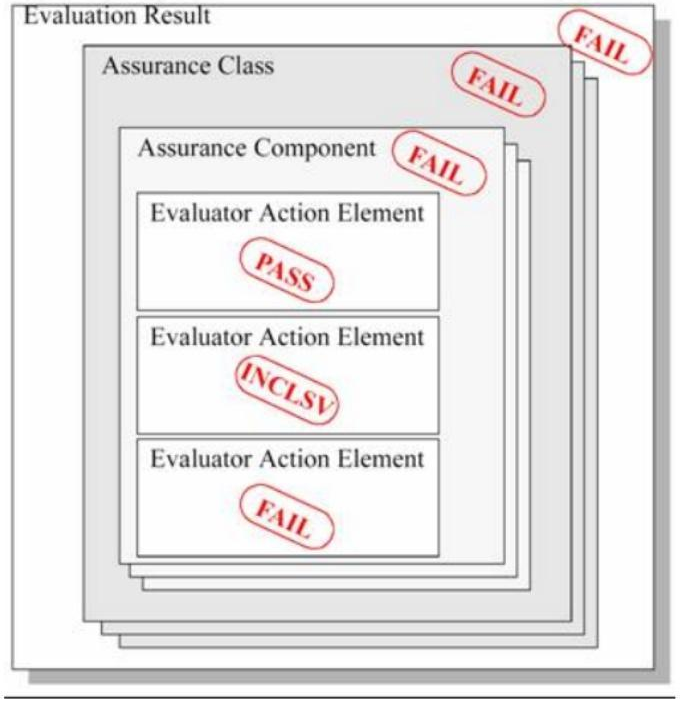
  → **SUMMARIZE THE EVALUATION PROGRESS INCLUDING THE STATUS AND DISPOSITION OF ISSUES AND COMMENTS REPORTED TO THE VENDOR**

- A final ETR is summited to the Scheme when all the evaluation activity work units have been completed

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

PHASE 3: RECOVER & FINALIZE
CERTIFICATION RECEPTION

- When the Scheme receives the final ETR from the CC evaluation lab the validators will:
  - → REVIEW/VALIDATE THE RESULTS
  - → ASK QUESTIONS TO THE EVALUATION LAB
  - → DECIDE WHETHER THE EVALUATION SUCCESSFULLY MET ALL OF THE REQUIREMENTS OR NOT.



© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Security Target

ITR ASE

SECURITY TARGET

ITR ASE

Extract of the certified **TrueCrypt** software document.
ST & ToE Reference + Declaration of conformity.

Ref. : ASE_INT.1.4C	**Verdict :** Pass

Requirement: "*The TOE overview shall summarise the usage and major security features of the TOE."*

Rationale:

ASE_INT.1-5

The information required is described by paragraph 1.3 and its sub-paragraphs :

The TOE is an on-the-fly data ciphering application on an IT support which allows data to be kept confidential and reduces the impact of loss in the event of theft of the equipment.

The main security characteristics are the ciphering and deciphering of data recorded on mass memory and read transparently from mass memory, after prior authentication. This paragraph states that the cryptographic keys are generated by the TOE, and that the importation of external keys is not envisaged.

The evaluator considers that the security target satisfies this requirement.

Ref. : ASE_SPD.1.2C	**Verdict :** Pass

Requirement: "*All threats shall be described in terms of a threat agent, an asset, and an adverse action."*

Rationale:

ASE_SPD.1-2

Threat is described in terms of a threat agent, an asset and an attack scenario :

- **Threat agent** : an attacker (from outside of the TOE's operational environment).
- **Asset** : sensitive user data stored on the disk.
- **Attack scenario** : recovery of one or more partial or total image(s) from the disk (possibly at different times) or after stealing the equipment or disk. In this security target, the attack can be broken down into the following scenarios :
  - The attacker discovers sensitive data with no confidentiality protection (absence of ciphering protection) ;

    The attacker succeeds in discovering the master key used to protect sensitive data by a symmetrical ciphering mechanism. He then uses this key to decipher and access the user's sensitive data.
  - The attacker succeeds in discovering the header key used to ensure that the master key is ciphered and protected (the master key is stored in the ciphered header). He then uses this header key to access the master key which enables the user's sensitive data to be deciphered ;
  - The attacker succeeds in discovering the authentication data (password and keyfiles) used to calculate the header key by derivation. He uses this data to access the header key, then the master key, and then the user's sensitive data.

SECURITY TARGET

ITR ASE

Extract of the certified **TrueCrypt** software document.
ST & ToE Reference + Declaration of conformity.

Réf. : ASE_REQ.2.4C	**Verdict :** Pass
Requirement: "*All operations shall be performed correctly.*"	
Rationale:	
ASE_REQ.2-5, ASE_REQ.2-6, ASE_REQ.2-7, ASE_REQ.2-8	
The evaluator has ensured that all the operations authorized by the Common Criteria (iteration, refinement, selection and allocation) on the functional requirements have been correctly carried out.	
He has particularly ensured that the refinements have been correctly identified and that they have been carried out in accordance with appendix C.4 of CC part 1.	

The verdicts determined by the evaluator for each element of each component are :

Element	Verdict
ASE_INT.1	Pass
ASE_CCL.1	Pass
ASE_SPD.1	Pass
ASE_OBJ.2	Pass
ASE_ECD.1	Pass
ASE_REQ.2	Pass
ASE_TSS.1	Pass

So, the final verdict coming from the results of the evaluator's activities associated with this class is : Pass.

Development Evidence

ITR ADV

Truecrypt

ITR ADV_FSP.4

This is an extract from the ADV_FSP documentation provided by the vendor for **Truecrypt**.

Ref. : ADV_FSP.4.4C	**Verdict :** Pass

Requirement : *"The functional specification shall describe all actions associated with each TSFI."*

Rationale :

ADV_FSP.4-6

The 'action' cells of the 4.x.1 tables associated with each service access interface clearly identify the list of associated actions for each interface.

Comment 1 (version 1.00) : The evaluator asked the developer to classify the TSFI actions into

- **SFR-enforcing actions,**
- **SFR-supporting actions,**
- **SFR-non-interfering actions.**

In response to this comment, the developer made the following modifications to the presentation of actions in paragraphs 4.x.1 :

- actions directly linked to SFRs (SFR-enforcing) are represented **in bold**,
- actions used to preserve the correct functioning of the first actions (SFR-supporting) are represented *in italics*,
- actions combining SFR-enforcing and SFR-supporting are represented ***in bold italics***,
- actions having no impact on the functioning (SFR-non-interfering) are left in normal script.

A mapping table added to paragraph 5 details for each TSFI the list of actions, and for each action the list of associated SFRs, detailing for each SFR if the relationship between the action and the SFR makes this SFR-enforcing or SFR-supporting. This table therefore makes it possible to classify actions into SFR-enforcing, SFR-supporting and SFR-non-interfering.

In addition, the evaluator compared the description of these actions with other elements present in the functional specifications. He also compared these elements to other evaluation material (design documents, architecture documents, user guides and implementation documents).

These analyses revealed no incoherence or incompleteness. The evaluator considers that the functional specifications are complete and precise : they fulfil this requirement satisfactorily.

Truecrypt - TOE Design

ITR ADV_TDS.3

This is an extract from the ADV_TDS documentation provided by the vendor for **Truecrypt**.

Ref. : ADV_TDS.3.1C	**Verdict :** Pass

Requirement : *"The design shall describe the structure of the TOE in terms of subsystems."*

Rationale :

ADV_TDS.3-1

The description in sub-systems provides a high-level description of what the various parts of the TOE do and how they do it. The description of the TOE in terms of sub-systems makes it possible to understand how it functions without having to know the implementation contents.

A description of the TOE in sub-systems is provided in paragraph 2 of the design document [ADV_TDS-2.00]. This paragraph presents a description of the TOE in sub-systems in graphic form (figure 1) and describes each of the sub-systems in table form.

The evaluator analysed this description of the TOE and compared it with the other available evidence. He confirms that all the sub-systems are well identified and that this description is coherent with the information contained in the other documents, particularly the security target and the user documentation.

The requirement is considered to be satisfied.

Truecrypt - IMPLEMENTATION REPRESENTATION

ITR ADV_IMP.1

This is an extract from the ADV_IMP documentation provided by the vendor for **Truecrypt**.

Ref. : ADV_IMP.1.1C	**Verdict :** Pass
Requirement : "*The implementation representation shall define the TSF to a level of detail such that the TSF can be generated without further design decisions.*"	
Rationale : **ADV_IMP.1-1** The source code is provided on the editor's web-site. The archive to download includes all the '.c' files as well as the '.sin' file, which enables the solution to be launched under Microsoft Visual Studio. Document [ADV_IMP-2.00] provides all the information which enables the TOE to be generated. After generating the TOE according to the instructions given, the evaluator confirms that the TOE can be generated without any other choice of design.	

Truecrypt - Security Architecture

ITR ADV_ARC.1

This is an extract from the ADV_ARC documentation provided by the vendor for **Truecrypt**.

Ref. : ADV_ARC.1.1C	**Verdict :** Pass
Requirement : *"The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document."*	
Rationale : **ADV_ARC.1-1** The [ADV_TDS-2.00] element describes the TOE in terms of sub-systems and modules. In the document which presents the security architecture ([ADV_ARC-2.00]), the level of detail is comparable to that used in the design description. The ADV_TDS.3 assurance component associated with the design of the TOE for the desired evaluation level demands that the security architecture's level of detail contains information which, when necessary, directly concerns implementation. The architecture document analysed presents this information directly in the form of source code elements when necessary. This information is judged satisfactory by the evaluator, as regards both level of detail and content.	

Truecrypt - Verdict Summary

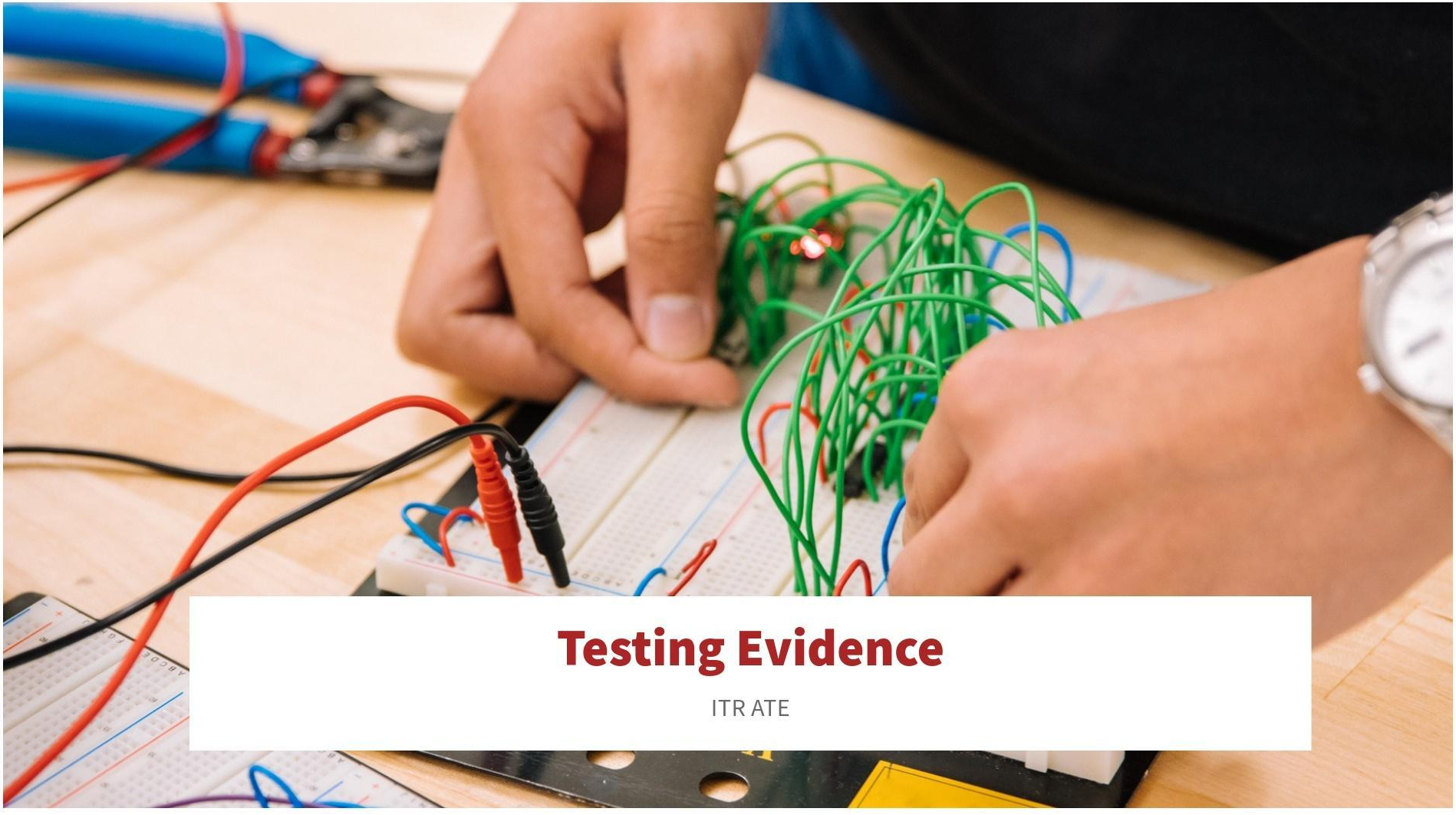
ITR ADV Evidence

This is an extract from the ADV_ARC documentation provided by the vendor for **Truecrypt**.

4.3. Summary of verdicts

32 The following table presents the results of the evaluation activities and sub-activity :

Element	Verdict
ADV_ARC.1	Pass
ADV_FSP.4	Pass
ADV_TDS.3	Pass
ADV_IMP.1	Pass



Testing Evidence

ITR ATE

Truecrypt - Functional Testing

ITR ATE_FUN.1

This is an extract from the ATE documentation provided by the vendor for **Truecrypt**.

Ref. : ATE_FUN.1.1C	**Verdict :** Pass

Requirement : *"The test documentation shall consist of test plans, expected test results and actual test results. "*

Rationale :

ATE_FUN.1-1

Chapter 2 of the [ATE-2.00] document presents the test plan, detailing the platform requires to carry out the tests, as well as the platform's hardware and software configuration.

Then, the test description (chapter 3) presents each test in the following form :

1-Function tested

1.1- Test XXX

1.1.1- Aim test

1.1.2- Prerequisite

1.1.3- Procedures

1.1.4- Expected results

Finally, chapter 4 presents the results obtained in table form featuring :

- The function tested
- Test identifier
- Expected results
- Results obtained
- Test conformity.

With regard to the tests formalised in chapter 3 of the test documentation [ATE-2.00] and the

Truecrypt - Samples
TEST COVERAGE (ITR ATE_COV.1)

Ref. : ATE_COV.1.1C	**Verdict :** Pass
Requirement : *"The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the interfaces in the functional specification."*	
Rationale : **ATE_COV.1-1** The table in chapter 5 of the [ATE-2.00] document presents the extent of test coverage on the TSFIs identified in the functional [ADV_FSP-2.00]. The 'Start TrueCrypt' and 'Quit TrueCrypt' TSFI tests were not formalised in the document, as they were considered irrelevant by the developer. In fact, these tests are unimportant and the evaluator therefore considers that it is not necessary to formalise them. The evaluator therefore considers that all the TSFIs are covered by the tests described in chapter 3 of the [ATE-2.00] document.	

	Relevance	Coverage	CREATE_01	CREATE_02	CREATE_03	CREATE_EXCEP_01	CREATE_EXCEP_02	CREATE_EXCEP_03	CREATE_EXCEP_04	MOUNT_01	MOUNT_02
Display information about a mounted encrypted disk	0	-1									
Display the drives corresponding to the	0	-1								1	1
file of a ciphered	1	3									
ttings	0	-1									
k	1	7	1	1	1	1	1	1	1		
	0	-1									
	0	-1									
	1	1									
isk	1	1									
and conformity outine	0	-1									
	1	1									
disk	1	1									
algorithm of a	1	3									
rd of a ciphered	1	3									
Mount a disk	1	3								1	1
Exit TrueCrypt	1	1									
Wipe cache password	1	2									
Backup volume header	1	1									
Restore volume header	1	1									

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

INDEPENDENT TESTS (ITR ATE_IND.2)

Ref. : ATE_IND.2.1C	**Verdict :** Pass
Requirement : "*The TOE shall be suitable for testing.*"	
Rationale : **ATE_IND.2-1** The version of the TOE supplied by the developer is identical to the one identified in the security target : TrueCrypt 4.2a. The configuration of the TOE, used to carry out the developer and evaluator tests, is the default configuration. **ATE_IND.2-2** The evaluator installed the TOE following the explanations in the user guide and the installation assistant. The TOE was installed and started up correctly.	

Ref. : ATE_IND.2.2C	**Verdict :** Pass
Requirement : "*The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.*"	
Rationale : **ATE_IND.2-3** A test platform was supplied by the developer. This platform is a PC composed of an AMD Athlon 64 X2, 3800+ processor and 1 Gb of RAM. The operating system is a Windows XP Pro Service Pack 2 32-bit version, default configuration. This test platform is identical to the machine used in the context of the developer's functional tests.	

A.1 Analysis of developer tests

Function Tested	Test Identifier	Results obtained by the developer	Results obtained by the evaluator	Conformity with developer tests
Create a ciphered disk	CREATE_01	TrueCrypt indicates that the ciphered disk has been successfully created.	Message confirming creation of ciphered disk.	Conforms
	CREATE_02	TrueCrypt indicates that the ciphered disk has been successfully created.	Message confirming creation of ciphered disk.	Conforms
	CREATE_03	TrueCrypt indicates that the hidden ciphered disk has been successfully created	Message confirming creation of hidden ciphered disk	Conforms
	CREATE_EXCEP_01	A window appears, indicating that the password is too short. TrueCrypt asks the user if he wishes to continue or change his password.	Warning that the password is too short. TrueCrypt gives the option to continue all the same, or to change the password.	Conforms
	CREATE_EXCEP_02	The 3 first password entries must be accepted. The fourth entry generates an error message that reminds the user which characters are authorised.	Only ASCII characters are authorised.	Conforms

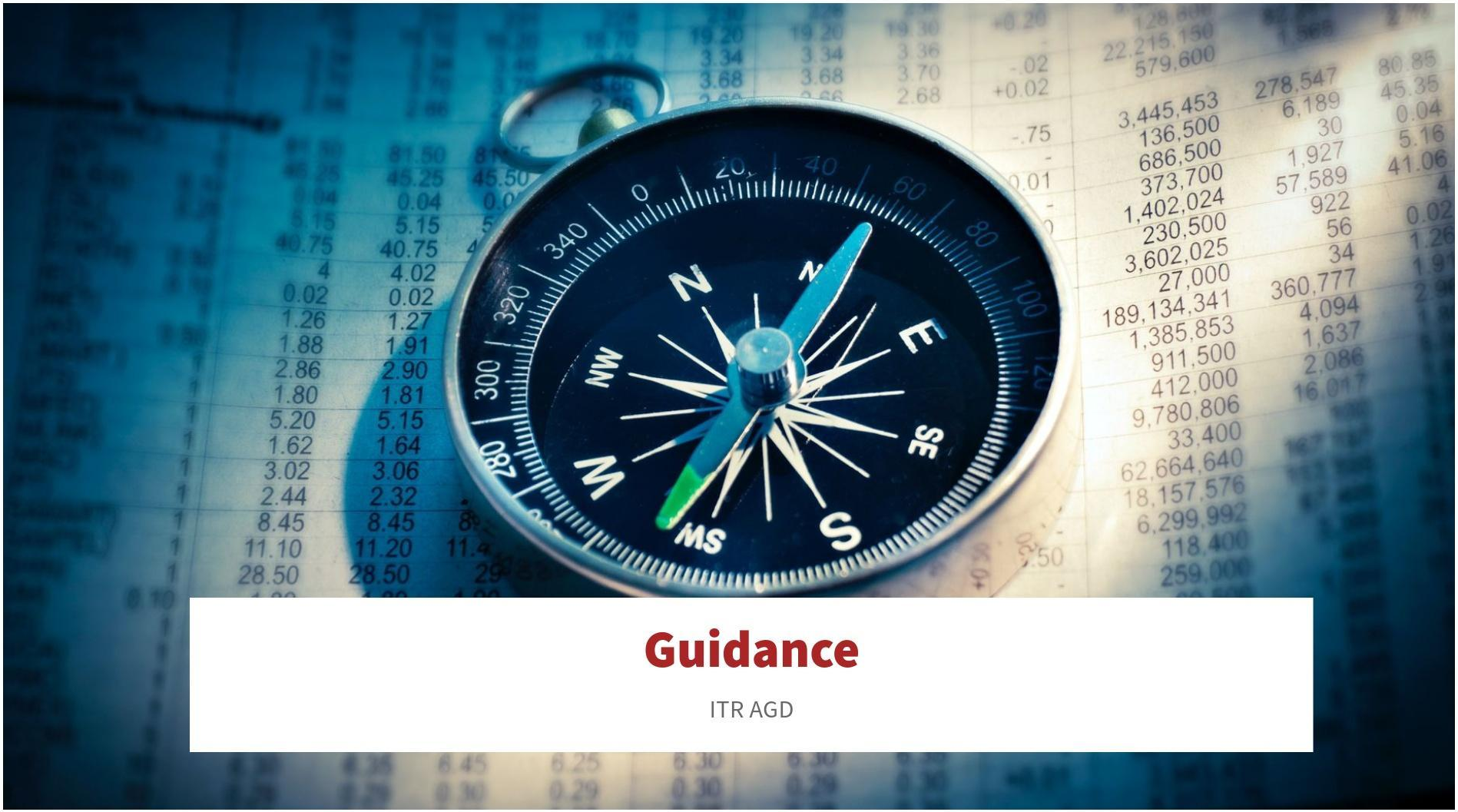
© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

4.3. Summary of verdicts

33 The following table presents the result of the evaluation activity and sub-activities:

Element	Verdict
ATE_COV.1	Pass
ATE_FUN.1	Pass
ATE_IND.2	Pass

So, the final verdict from the results of the evaluator's activities associated with this class is: Pass.



Guidance

ITR AGD

Truecrypt - Samples
OPERATIONAL GUIDANCE (AGD_OPE)

Ref. : AGD_OPE.1.3C	**Verdict :** Pass

Requirement : *"The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate."*

Rationale :

AGD_OPE.1-3

The 'Introduction' chapter of the TrueCrypt documentation presents the use and the main functionalities of the software.

Then, each functionality is described precisely so that the user can use the various interfaces correctly.

For example, the 'Beginner's Tutorial' chapter explains step by step how to create a volume. It is structured as follows :

- an introduction which gives the user information about the purpose of the interface : *This chapter contains step-by-step instructions on how to create, mount and use a TrueCrypt volume*
- a step-by-step explanation composed of screen copies and explanatory texts describing methods for displaying the interfaces and the various parameters which can be used.

The 'Command Line Usage' chapter gives the user precise explanations on the various commands which can be used to display the interfaces.

As we saw in the previous criterion, the instructions for the TrueCrypt service access interfaces are in the documentation.

The evaluator states that the TSF described in the functional specification document is indeed coherent with the user guide.

The guide is comprehensive enough for a user to use the available TSFIs in a secure manner.

Ref. : AGD_OPE.1.1E	**Verdict :** Pass

Requirement : "*The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.*"

Rationale :

Comment 1 (version 1.00) : The evaluator considers that the information provided does not fully satisfy the content and evidence presentation requirements (see the Rationale in the AGD_OPE.1.6C elementary task).

The verdict cannot therefore be pass.

Following the modification of the user guide, the evaluator confirms that the information provided satisfies the content and evidence presentation requirements.

3.1.4. Verdict on the component

15 Summary of verdicts :

Element	Verdict
AGD_OPE.1.1C	Pass
AGD_OPE.1.2C	Pass
AGD_OPE.1.3C	Pass
AGD_OPE.1.4C	Pass
AGD_OPE.1.5C	Pass
AGD_OPE.1.6C	Pass
AGD_OPE.1.7C	Pass
AGD_OPE.1.1E	Pass

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

TOOLS & TECHINQUES (ALC_TAT.1)

Ref. : AGD_PRE.1.1E	**Verdict :** **Pass**
Requirement : "*The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.*"	
Rationale : The evaluator confirms that the information provided satisfies the content and evidence presentation requirements.	

Ref. : AGD_PRE.1.2E	**Verdict :** **Pass**
Requirement : *"The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation."*	
Rationale : **AGD_PRE.1-5** Having implemented the installation procedure, the evaluator states that it allows the TOE to be prepared in conformity with requirements.	

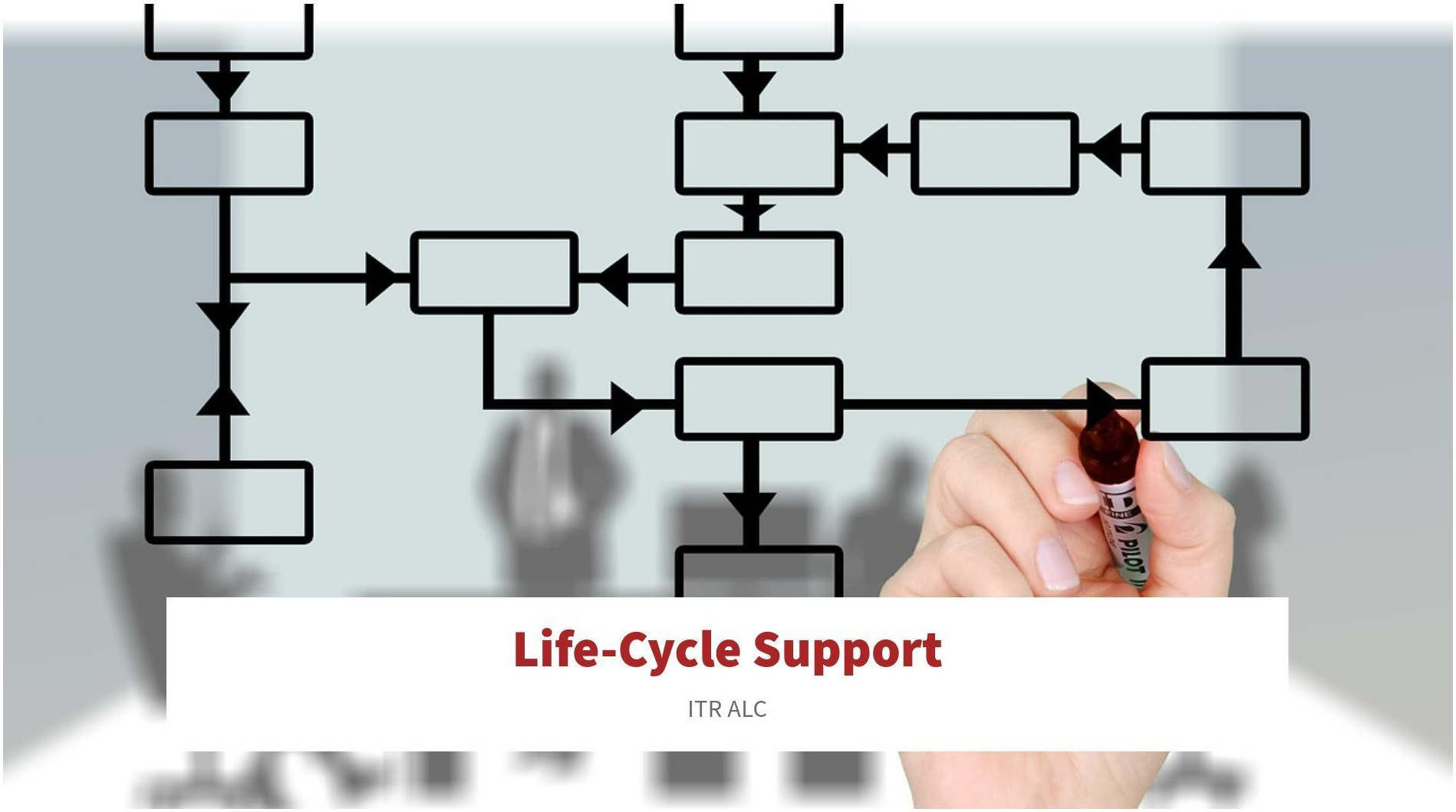
3.2.4. Verdict on the component

20 Summary of verdicts :

Element	Verdict
AGD_PRE.1.1C	***Pass***
AGD_PRE.1.2C	***Pass***
AGD_PRE.1.1E	***Pass***
AGD_PRE.1.2E	***Pass***

All verdicts given for the component lead us to apply a **Pass** verdict for the AGD_PRE.1 component.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED



Life-Cycle Support

ITR ALC

CONFIGURATION MANAGEMENT SCOPE (ALC_CMS)

3.2.2. Content and presentation of evidence

Ref. : ALC_CMS.2.1C	**Verdict :** Fail
Requirement : "*The configuration list includes the following: the TOE itself; the evaluation evidence required by the SARs in the ST; and the parts that comprise the TOE."*	
Rationale : **ALC_CMS.2-1** **As there is no configuration items list, the evaluator cannot carry out any verification. This task cannot be carried out.**	

Ref. : ALC_CMS.2.2C	**Verdict :** Fail
Requirement : *"The configuration list shall uniquely identify the configuration items."*	
Rationale : **ALC_CMS.2-2** **As there is no configuration items list, the evaluator cannot carry out any verification. This task cannot be carried out.**	

3.2.4. Verdict on the component

25 Summary of verdicts :

Element	Verdict
ALC_CMS.2.1C	***Fail***
ALC_CMS.2.2C	***Fail***
ALC_CMS.2.3C	***Fail***
ALC_CMS.2.1E	***Fail***

26 All verdicts given for the component lead us to apply a **Fail** verdict for the ALC_CMS.2 component.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

CONFIGURATION MANAGEMENT (ALC_CMC)

Ref. : ALC_CMC.2.3C	**Verdict :** **Fail**
Requirement : *"The CM system shall uniquely identify all configuration items. "*	
Rationale : **ALC_CMC.2-4** According to the various exchanges with the 'TrueCrypt Foundation', it uses the *CVS* configuration management system. However a migration towards *Perforce* should be carried out in the future. **As no evidence is available, this task cannot be satisfied.**	

3.1.3. Evaluator tasks

Ref. : ALC_CMC.2.1E	**Verdict :** **Fail**
Requirement : "*The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.*"	
Rationale : **As the evaluator has no document relating to configuration management, he cannot give a Pass verdict.**	

3.1.4. Verdict on the component

19 Summary of verdicts :

Element	Verdict
ALC_CMC.2.1C	***Pass***
ALC_CMC.2.2C	***Fail***
ALC_CMC.2.3C	***Fail***
ALC_CMC.2.1E	***Fail***

20 All verdicts given for the component lead us to apply a **Fail** verdict for the ALC_CMC.2 component.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

DELIVERY PROCEDURES (ALC_DEL.1)

Ref. : ALC_DEL.1.1E	**Verdict :** **Pass**
Requirement : "*The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.*"	
Rationale : **Comment 1 :** The evaluator considers that the information provided cannot fully satisfy content and evidence presentation requirements. The verdict cannot be Pass. Following the replies given by the developer, the evaluator considers that the information supplied fully satisfies the content and evidence presentation requirements.	

3.3.3. Verdict for the component

30 Summary of verdicts :

Element	Verdict
ALC_DEL.1.1C	***Pass***

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Life-Cycle ITR summary

4.3. Summary of verdicts

41 The following table presents the result of the evaluation activity and sub-activities:

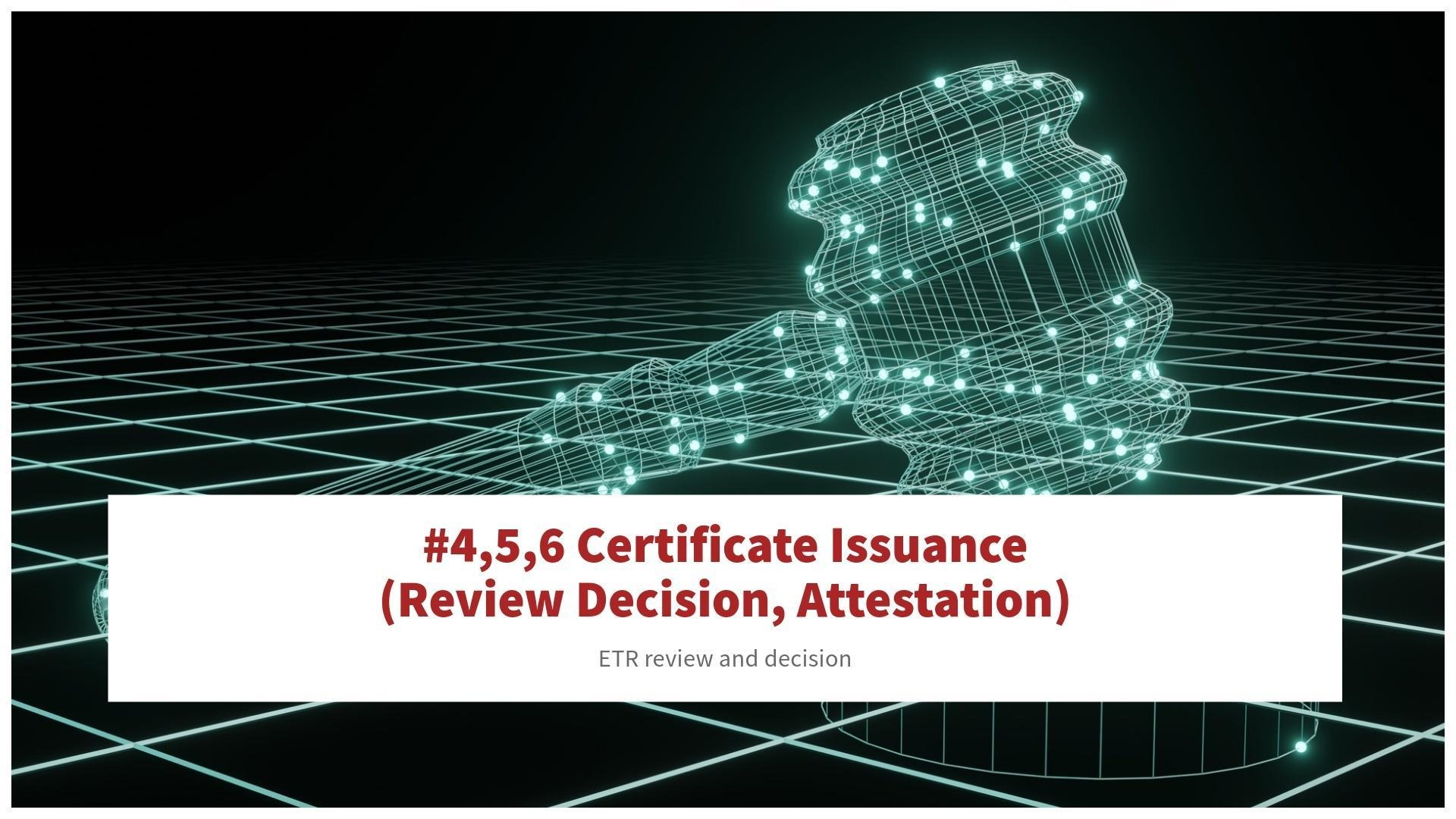
Element	Verdict
ALC_CMC.2	**Fail**
ALC_CMS.2	**Fail**
ALC_DEL.1	**Pass**
ALC_TAT.1	**Inconclusive**

42 So, the final verdict from the results of the evaluator's activities associated with this class is : **Fail**.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED

Vulnerability Analysis

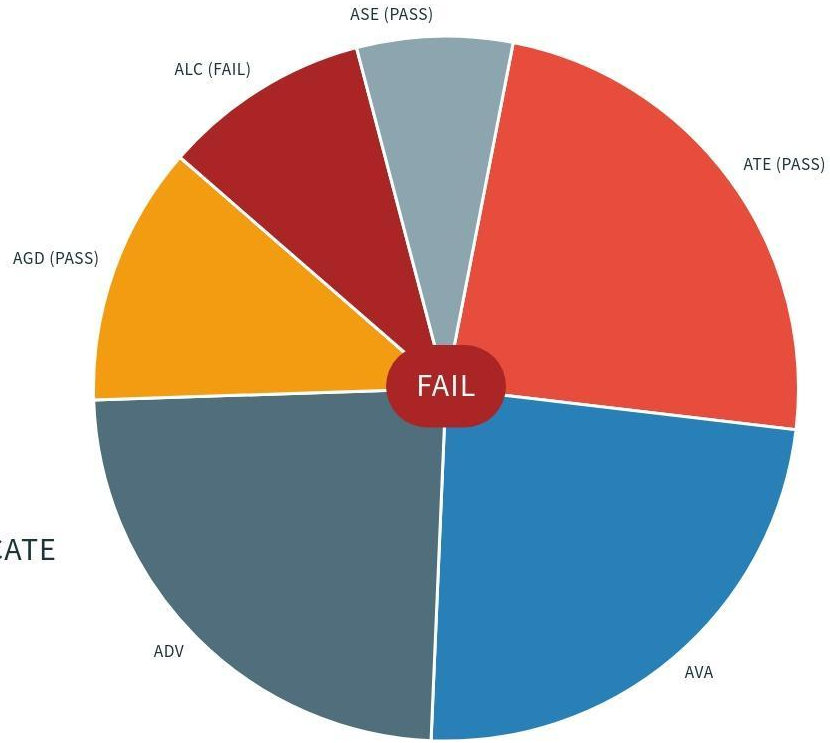
ITR AVA



#4,5,6 Certificate Issuance (Review Decision, Attestation)

ETR review and decision

DECISION



NO CERTIFICATE ISSUANCE

©2025 Proprietary and Confidential. All Rights Reserved.

RED ALERT LABS
IoT Security

CERTIFICATE CONTENT

1 | IDENTIFICATION

2 | SECURITY POLICIES

3 | ASSUMPTIONS AND CLARIFICATION OF SCOPE

4 | ARCHITECTURAL INFORMATION

5 | SUPPLEMENTARY CYBERSECURITY INFORMATION

6 | ICT PRODUCT TESTING

7 | RESULTS OF THE EVALUATION AND INFORMATION REGARDING THE CERTIFICATE

8 | SUMMARY OF THE SECURITY TARGET

9 | **WHEN AVAILABLE, MARK OR LABEL ASSOCIATED TO THE SCHEME**

10 | BIBLIOGRAPHY

©2025 Proprietary and Confidential. All Rights Reserved.

RED ALERT LABS
IoT Security

MARK / LABEL

OVERARCHING ECCF LABEL

Demo Label

Elements to be added for the EUCC scheme:

1. EUCC logo
2. QR code (link) to Enisa ECCF website
3. CSA assurance level (substantial – high)
4. Vulnerability Evaluation Level (AVA_VAN)
5. Sentence: "certified in European Union"

ECCF Logo *	EUCC Logo *
Certified in the European Union 	ECCF Enisa website 
CSA – Assurance Level (substantial / high)	Vulnerability Evaluation Level AVA_VAN

* Logo and rules for its usage to be developed by the entity that registers the respective logo.

#7 Certificate Maintenance

Assurance Continuity & IAR

PHASE 3: RECOVER & FINALIZE
RE-CERTIFICATION/ASSURANCE CONTINUITY

ASSUMPTION

CC certificates are only valid for a single version of a product.

GOAL

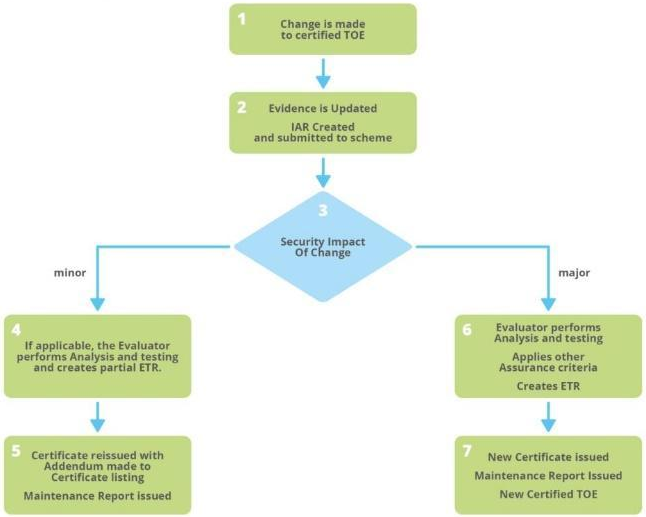
Shorten the re-evaluation cycle for previously evaluated product

HOW TO DO ?

Provide evidence that changes in the newer version of the product do not compromise the security claims and evidence presented in the prior version's evaluation.

An Impact Analysis Report (IAR) is submitted to the same evaluation lab that performed the original evaluation.

© 2020 RED ALERT LABS – ALL RIGHTS RESERVED



©2025 Proprietary and Confidential. All Rights Reserved.

RED ALERT LABS
IoT Security

IAR table of content

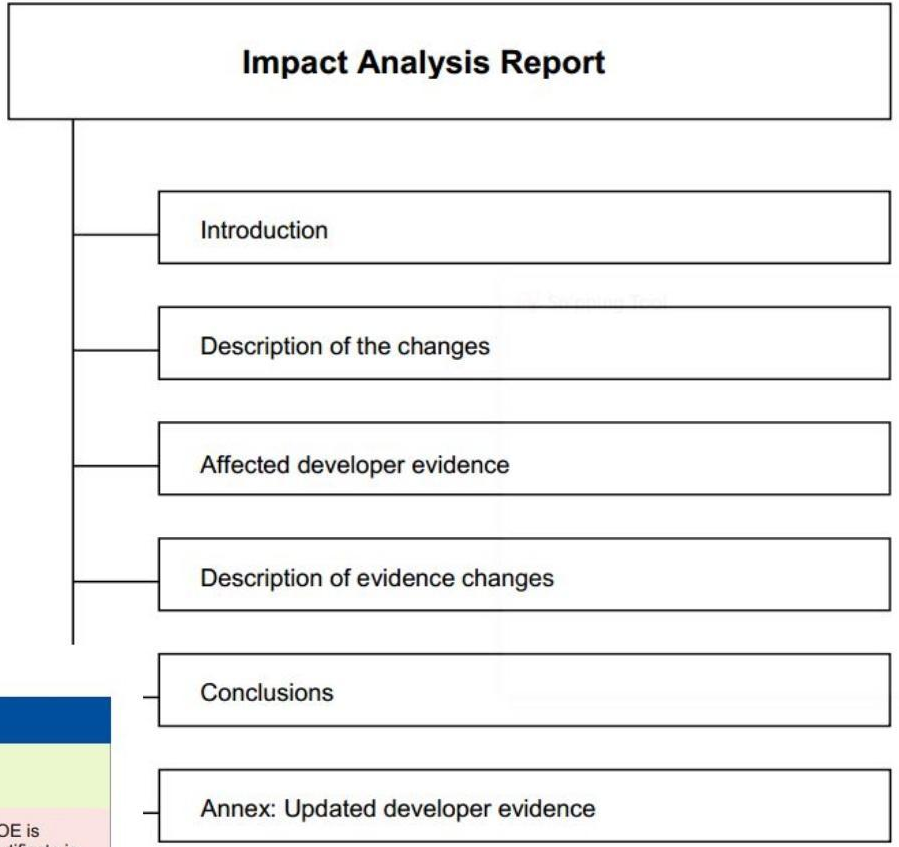


Table 1: Impact of re-assessement results on certificates

Re-assessment results	Impact on the certificate
Positive[66]	The validity of the initial certificate is extended into the renewed certificate.
Negative	The new AVA_VAN level reached by the re-assessed TOE is indicated into a re-issued certificate, and the previous certificate is archived.

THANK YOU