Netherlands Scheme for Certification in the Area of IT Security (NSCIB)

Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB)

NSCIB Scheme Instruction 09

Clarification of the TSFI concept

Approved.....

Technical Manager NSCIB

Instruction	09
Report title	Clarification of the TSFI concept
Date of issue	November 15th, 2012
Version	1.0
Distribution	Public
Filename	NSI_10_Clarification_of_the_TSFI concept_v1.0.doc

TÜVRheinland®
Precisely Right.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

1 Purpose of this document

The purpose of this document is to clarify the concept of TSFI.

2 TSFI definition

The definition of TSFI in CC Part 1 is clarified to[1]:

TSF interface (TSFI): a means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF**, such that:**

- **Attackers can possibly access this means, and/or**
- **SFRs are traced to this means**

For the purpose of this definition:

- An attacker is any external entity or non-TSF subject in the TOE that has not been explicitly defined as trusted in the ST
- An attacker can possibly access a means unless either the TSF itself, or the security objectives for the operational environment, or a combination thereof, prevents the attacker from having access.

Examples:

- A physical console of a server that can be accessed by both trusted and non-trusted administrators is a TSFI regardless of whether SFRs trace to it.
- A physical console of a server that only trusted administrators have access to, and no SFRs trace to it, is not a TSFI
- A physical console of a server that only trusted administrators have access to, and FMT_SMF.1 traces to is a TSFI
- The PCB of a security module that is claimed to meet FPT_PHP.* (and where the physical enclosure encompasses the PCB) is not a TSFI.
- The physical enclosure of the security module above is a TSFI

3 Splitting of means

In some cases, a developer may want to split a means into two parts, where part of the means is a TSFI, while another part of the means is not a TSFI. This allows the developer to separate the TSFI from the remainder of the means, to make his documentation burden smaller, as he only has to document the TSFI in depth, and not the entire means.

Examples include:

- The physical layer and datalink layer of a firewall, consisting of both hardware and software, where the security objectives of the environment state that the only attackers reside on the Internet, are not TSFI, as these two layers cannot be directly addressed from the Internet. However, the network layer and higher layers are TSFI. Splitting the “network interface” into two parts would be beneficial, as the developer would not have to specify the physical and datalink layers in depth.
- An encrypted IP connection between the TSF and a trusted server over an untrusted network is a TSFI as attackers have access to it. Splitting the interface into:
  - A TSFI specifying the encryption supplied by the TSF (which could be attacked)
  - A non-TSFI interface specifying the traffic between TSF and backup server running over the encryption[2]

[1] Additions are in **bold**

[2] This interface is not accessible to attackers unless the encryption is successfully attacked first, which would already break the SFRs.

would be beneficial, as the developer would not have to specify the backup protocol in depth.

4 Changes required to other parts of the CC

CC Part 3 Annex A.2 is to be considered secondary to this interpretation. That is, where this instruction and CC Part 3 Annex A.2 are in conflict, this instruction has precedence.

There are no further changes: all other CC activities are unaffected.