Protection Profile for Peripheral Sharing Switch

13 February 2015

Version 3.0

Table of Contents

LIST OF FIGURES

List of Tables

1. INTRODUCTION

This Protection Profile (PP), describing security requirements for a Peripheral Sharing Switch (PSS), defined to provide a mechanism to securely connect a common set of peripherals to the attached computer(s), is intended to provide a minimal, baseline set of requirements that are targeted at mitigating well-defined and described threats. It represents an evolution of “traditional” Protection Profiles and the associated evaluation of the requirements contained within the document. This introduction will describe the features of a compliant Target of Evaluation (TOE) and will also discuss the evolutionary aspects of the PP as a guide to readers of the document. Glossary and acronyms are defined in Annex A.

1.1. PP Reference Identification

PP Reference: Protection Profile for Peripheral Sharing Switch (PSS)

PP Sponsor: National Security Agency (NSA)

PP Version: 3.0

PP Date: February 12, 2015

1.2. Technical Definitions

Term	Meaning
Administrator	A person who administers (e.g. installs, configures, updates, maintains) a system of device(s) and connections.
Configurable Device Filtration (CDF)	PSS function that qualifies (accepts or rejects) peripheral devices based on field configurable parameters.
Combiner	A PSS switch with video integration functionality.
Connected Computer	A computing device (platform) connected to the PSS. May be a personal computer, server, tablet or any other computing device with user interaction interfaces.
Connection	Enables devices to interact through respective interfaces. It may consist of one or more physical (e.g. a cable) and/or logical (e.g. a protocol) components.
Device	An information technology product with which actors (persons or devices) interact.
Display	A Human Interface Device (HID), such as a monitor or touchscreen,

	which displays user data.
External Entity	An entity outside the TOE evaluated system, its connected computers and its connected peripheral devices.
Fixed Device Filtration (FDF)	PSS function that qualifies (accepts or rejects) peripheral devices based on fixed parameters.
Human Interface Device (HID)	A device that allows for user input. For example, keyboard and mouse.
Interface	Enables interactions between actors.
Isolator	A PSS with a single connected computer.
Keyboard	A Human Interface Device (HID) such as a keyboard, keypad or other text entry device.
KM	A PSS that switches only the keyboard and pointing device.
Non-Selected Computer	A connected computer not currently selected by the PSS user.
Peripheral	A device that exposes an actor's interface to another actor.
Peripheral Group	An ordered set of peripherals.
Pointing Device	A Human Interface Device (HID), such as a mouse, track ball or touch screen (including multi-touch).
Selected Computer	A connected computer currently selected by the PSS user.
User	A person or device that interacts with devices and connections.
User Authentication Device	A peripheral device used to authenticate the identity of the user, such as a smart-card reader, biometric authentication device or proximity card reader.
Video Wall	Consists of multiple computer monitors, video projectors, or television sets tiled together contiguously or overlapped in order to form one large display.

Table 1: Technical definitions

1.3. Compliant Targets of Evaluation

Compliant targets of evaluation typically switch multiple peripherals to multiple computers based on the user switching inputs. Authorized switching methods may be implemented locally on the PSS front panel. Note that authorized switching methods specifically do not include the following methods: keyboard shortcuts, also known as “hotkeys”, automatic scanning, and voice activation. Note that this PP is also applicable to TOEs that support one computer only (isolator). The primary function of the PSS is to provide isolation between computer sources and peripherals. It is a tool to share peripheral devices. The same security goals are applicable even when there is only one computer involved. There may be a requirement to provide isolation between the computer and the peripheral devices and in that case, a single port PSS, or isolator, may be used. Compliant TOEs support one or more authorized switching methods, which are Push-buttons, tact switches, Toggle switches, Touch-screen, Mouse or cursor control.

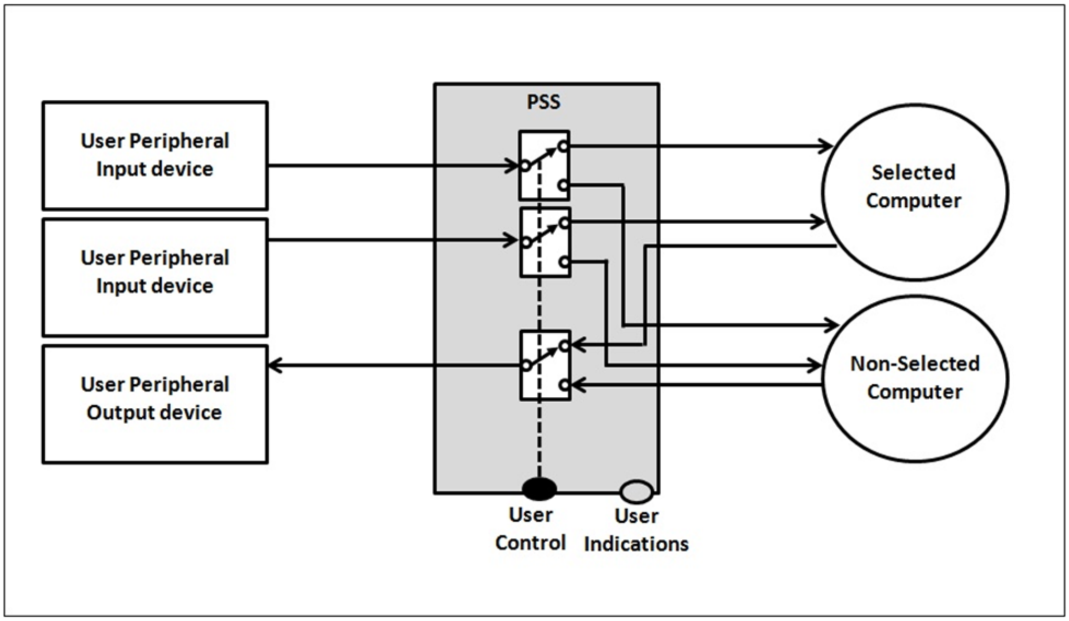

PSS
User Peripheral Input device
User Peripheral Input device
User Peripheral Output device
Selected Computer
Non-Selected Computer
User Control
User Indications

Figure 1: Simplified PSS Block Diagram

1.4. TOE Background

In the context of this PP, a peripheral sharing switch provides a mechanism to securely connect a common set of peripherals (1 to n) to the attached computer(s) (1 to j) without sharing or transferring data (Figure 1). The PSS will follow a deliberate action from the user to enable an interaction between the connected peripherals and the selected computer. Examples of the type of PSS that should claim compliance to this PP include keyboard, video, mouse (KVM) switches; keyboard, mouse (KM) switches; isolators (PSS with a single connected computer); and combiners (PSS capable of displaying multiple computers in one video display). Examples of devices that are not suitable for evaluation against this PP include Internet Protocol (IP) and network-attached switches and matrix switches. Basic use cases are defined in Annex B.

1.5. TOE Scope

While the functionality that the TOE is obligated to implement (in response to the described threat environment) is discussed in detail in later sections, it is useful to give a brief description here. Compliant TOEs will provide security functionality that addresses threats to the TOE and implements policies that are imposed by law or regulation.

This assurance standard specifies information security requirements for Peripheral Sharing Switch for use in an enterprise. A PSS device in the context of this assurance standard is a device which is composed of one or more hardware components or platforms and its software or firmware. It may include cables and accessories, if applicable.

Connected peripheral devices, computer platforms or extenders are not covered under this PP and may be covered by another PP, if applicable. Nevertheless, testing of the TOE requires a complete setup that includes computers and peripheral devices.

PSS devices covered by this PP:

- may consist of one or more connected sub-systems (for example one KM switch and one video switch);
- may switch multiple instances of the same type of peripheral device (for example PSS may support multiple displays);
- may have a subset of the switching functions (for example display switching only);
- may support newer protocols (unlike previous PSS PP);
- may be controlled by newer user controls (for example multi-touch windows);

For additional details regarding use cases for the PSS see Annex B of this PP.

2. SECURITY PROBLEM DESCRIPTION

The security problem to be addressed by compliant TOEs is described by threats and policies that might be targeted at the specific functionality of a PSS. The following sections detail the problems that compliant TOEs will address.

2.1. Cross-Computer Flow

Peripheral Sharing Switches (PSS) are at high risk of a targeted attack as they are often used to support users operating over wide security gaps. If a remote attacker can access a computer connected to a PSS, then a targeted attack may be launched in an attempt to access the other connected computer or network via the PSS.

PSS may also be deployed across networks with similar security levels, which must be isolated to maintain security and availability.

The most critical threat affecting a PSS is an intentional attack designed to leak data between two connected computers. A remote attacker may abuse one hacked computer connected to the PSS in an attempt to inject code or data onto the other connected computer or network. Alternatively, an attacker may attempt to leak data from the one side of the PSS to the hacked computer on the other side of the TSS (and from there to the remote attacker).

Shared peripheral devices may be exploited to temporarily store data while switched between computers. It is assumed that all standard connected peripheral devices are vulnerable to data retention through documented or undocumented memory space. For example, an attacker could exploit display Plug and Play signals (e.g., extended display identification data (EDID) or Video Electronics Standards Association (VESA) Monitor Control Command Set (MCCS)) to store target data payloads while the PSS is switched to the targeted computer or network, and then later download this data payload while the display is switched to the other computers or networks. The leaked data payload may be later collected, encrypted and sent to the remote attacker site through various channels such as web access, emails, or IP telephony.

Data may also be leaked between computers across the PSS via various signaling methods. Signaling methods refer to the use of simple bit-by-bit effects used to transfer data across the PSS while in use or while the PSS is being switched between computers. Signaling may use electrical leakages across computers or some other event that may be sensed at the other side of the PSS. For example, if one computer connected to the PSS is attempting to power cycle its USB (Universal Serial Bus) port power and another computer connected to the PSS senses these power changes through another port host interface, data may be leaked across these computers.

It should be noted that the data leaked from the PSS in these cases may be unrelated to the data entered or received by the specific user. Data may leak through the PSS without user awareness when the user is performing normal operational tasks or while the PSS is left powered on and unattended.

It should also be noted that the scope of threats in this PP are limited to threats that are reasonably within the physical and design limitations of standard computers. It is assumed that connected computers are standard personal computer (PC) platforms with no special analog, video, or data collection cards or peripherals. For example, video signal leakage through the PSS between the user-selected computer and a non-selected computer is not considered as a reasonable threat as not all standard PCs are capable of analyzing and digitizing a weak cross-talk signal or a full strength signal.

This PP does not cover TEMPEST threats and it is assumed that the computers connected to the PSS as well as the peripheral devices are not TEMPEST approved. Also, it should be noted that the PSS applicable to this PP are expected to have a common ground plane / grounded enclosure that will short all connected computer ground planes.

A subset of the data leakage threat is the special case of user data (e.g., text entered via keyboard) or residual user data that is leaked to a computer connected to the PSS, but not selected.

Threat	Definition
T.DATA_LEAK	A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.

Table 2: Cross computer flow threats

2.2. Unintended Switching

Peripheral Sharing Switches allow the user to switch between connected computers. Unintended switching is a security threat in which data could be routed to the wrong connected computer without the user’s knowledge. For example, keyboard shortcuts are often used in commercial switches to switch to another channel. If a user inadvertently presses a keyboard shortcut combination, the user could be typing on a channel other than the one to which the user intended to connect. In an environment where the PSS is used to connect computers of differing classifications, the situation becomes a critical threat that must be mitigated. Therefore, the use of keyboard shortcuts, or “hotkeys” should be disallowed. Similarly, a scanning function is commonly used in commercial switches. This feature is also a security threat and should be disallowed.

To address the unintended switching threat, the PSS must:

1. Require a deliberate user action to switch between connected computers, and
2. Provide a continuous visual indication of the computer to which the user is connected.

Traditionally, the method of “deliberate action” from the user was push-button switching. While this method is still acceptable and the most widely used, other methods have gained popularity as technology has evolved. These methods include use of a touch screen, mouse or cursor control. It should be noted that the user must always have line-of-sight (LoS) to either the PSS itself or to the switching mechanism.

Visual indication has traditionally been handled by light-emitting diode (LED) indicators on the front panel of the PSS. Other acceptable indication methods include lighted push-buttons, graphic or text displays, and on-screen displays (OSDs). If a display is used, it must be “always on” to ensure that continuous indication is provided.

Threat	Definition
T.UNINTENDED_SWITCHING	A threat in which the user is connected to a computer other than the one to which the user intended to be connected.

Table 3: Unintended switching threat

2.3. Peripheral Device Threats

Peripheral device threats can be divided into two areas:

1. *Unauthorized peripheral device threats* – threats imposed by peripheral devices that should not be connected to the specific PSS port (e.g., a user might connect a mass storage device to the PSS console keyboard port).
2. *Authorized but untrusted peripheral device threats* – threats imposed by legitimate and authorized peripheral devices while being used with the PSS, as all standard authorized peripheral devices connected to the PSS may be untrusted (e.g., a standard USB keyboard with a firmware update endpoint may be used to leak data when switched by the PSS).

Unauthorized Peripheral Device Threats

Peripheral devices that are not authorized for use in a specific PSS port may cause security breaches such as data theft or data leakage. Also, each PSS peripheral port should have an approved list of authorized peripheral devices. Annex C of this document contains the PSS authorized peripheral devices list.

Authorized But Untrusted Peripheral Device Threats

For the purpose of this PP, it may be assumed that all standard authorized peripheral devices (based on Annex C of this document) are untrusted. The term “standard” in the context of this PP means commercial off-the-shelf peripherals and does not cover special purpose high-security peripherals that may be used as well. The PSS must be designed to securely operate with all peripheral devices and therefore, the PSS must mitigate the potential threats of all authorized peripheral devices.

It should be noted that standard peripheral devices may be secure and trusted in operation with other types of equipment; however, the use of these devices with a PSS may exploit severe data leakage threats.

Threat	Definition
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.

Table 4: Peripheral device threats

2.4. Audio Threats

Audio threats in PSS may be resulted from the following:

1. *The user intentionally or unintentionally connects a microphone to the PSS*. A microphone may be misused by a hacked connected computer to leak data or voice (audio eavesdropping) to a remote site.
2. The user uses an audio output device (for example – headphones) that may be misused as a microphone, enabling a remote attacker to perform audio eavesdropping in the vicinity of the TOE.

The audio CODEC used in most PCs and portable devices is a highly flexible analog signal processor. It can amplify and filter a weak signal and, in many cases, it can be switched to multiple physical ports through software. If one computer connected to the TOE is hacked by a remote attacker, that computer may also be misused to provide audio eavesdropping in the vicinity of the TOE.

It is also possible to use that computer to “listen” to audio being played by another hacked computer on a different network, bridging the air-gap between the two networks and leaking data through audio signaling.

Another well-known threat is the misuse of audio output devices such as headphones to work as a low-gain dynamic microphone. All dynamic headphones are very similar to microphones (moving coil and static magnet). With proper amplification, the weak signal generated by these devices can be used for audio eavesdropping around the TOE.

It should be noted here that amplified speakers are not vulnerable to this type of threat as the amplifier serves to provide isolation for the weak reverse signal and attenuates it below usable levels.

It also should be noted that digital audio passed through the video (for example in HDMI) or passed through separate lines is not a concern, since it does not introduce analog signal leakage vulnerabilities.

Threat	Definition
T.MICROPHONE_USE	Microphone connected to the TOE used for audio eavesdropping or to transfer data across an air-gap through audio signaling.
T.AUDIO_REVERSED	Audio output device used by an attacker as a low-gain microphone for audio eavesdropping. This threat is an abuse of the computer and TOE audio output path to reverse the analog data flow from the headphones to the computer. The computer then amplifies and filters the weak signal, and then digitizes and streams it to another location.

Table 5: Audio threats

2.5. Device Tampering

Tampering (i.e., replacement or modification) of a PSS can be detrimental to the enforcement of the intended security policies. Unauthorized replacement of a PSS could occur during shipment, storage, or even when in use, depending upon the specific circumstances and degree to which attackers may have access. If the user cannot determine that the correct device has been received, or the user is unable to identify when a device in use may have been replaced, the user may inadvertently use a PSS that does not enforce the required or expected security policies.

PSS tampering could involve physical modifications to the PSS device or logical modifications accomplished via the various PSS connectors.

The physical tampering of a PSS is comparable to PSS replacement and could also occur at any time (e.g., shipping, storage and use). If physical PSS tampering is not identified, the entire PSS logic could be replaced and physical connections, controls, and indicators could be altered. Ultimately, if physical tampering occurs and goes unidentified the PSS may no longer enforce the required or expected security policies.

Logical tampering of a PSS is effectively comparable to PSS replacement. If tampering occurs and goes undetected, the PSS security-enforcing functions may have been modified such that the PSS may no longer enforce the required or expected security policies. Logical tampering might involve modifying the PSS firmware (e.g., during the firmware update process) to effect a permanent change in the PSS. Alternately, logical tampering might involve modification (e.g., via a buffer overrun attack) of in-memory code or data structures to effect a temporary change in the PSS. Such attacks could be launched from an attached computer, peripheral, or via some other connection (e.g., debug ports) under the control of a malicious user. It should be noted that the malicious user may be the local PSS user or a remote user who attempts to attack the organization from a remote location.

Threat	Definition
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code embedded in the TOE's volatile or non-volatile memory to allow unauthorized information flows between connected devices.
T.PHYSICAL_TAMPER	A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.REPLACEMENT	A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.

Table 6 – Device tampering threats

2.6. Unsafe Failure

A catastrophic PSS failure may cause data leakage across its connected computers; therefore, the PSS design must minimize the potential of an undetected catastrophic failure. Other less critical PSS failures may weaken or disable security mechanisms, leaving the PSS vulnerable to attacks or misuse that in turn may cause data leakages.

Data leakage through the PSS may cause significant damage to the operating organization as it may operate undetected for a long time. Damage potential may be higher if the security gap across the PSS is wide (e.g., National security to Internet), or if the security level of the computers connected is high. Even across the same security level (i.e., network segmentation), the damage potential is high as penetration into one network may assist the potential attacker in further penetrating another targeted network through a breached PSS connected between these networks.

Also, if the PSS switching mechanism fails, the PSS should prevent an unintended switching condition. For example, if a push-button is stuck, the PSS may behave as if it is in scanning mode and the user may be confused as to which computer is selected, resulting in a security threat similar to the keyboard shortcut example discussed previously.

Threat	Definition
T.FAILED	Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

Table 7 – Unsafe failure threat

3. SECURITY OBJECTIVES

Compliant TOEs will provide security functionality that addresses threats to the TOE and implements policies that are imposed by law or regulation. The following sections provide a description of this functionality with respect to the threats previously discussed that necessitate inclusion in compliant TOEs. The security functionality provided includes protected communications to and between elements of the TOE; administrative access to the TOE and its configuration capabilities; system monitoring for detection of security relevant events; and the ability to verify the source of updates to the TOE.

3.1. Data Flow Isolation

A compliant TOE must be designed and tested to minimize the risk of unauthorized data flow and to properly protect the TOE and/or its connected peripheral devices from being exploited in an attempt to leak data. A compliant TOE computer interface shall be isolated from all other TOE computer interfaces.

Annex D contains data flow illustrations for reference.

See Annex D, Table 1, Flows J and K. The TOE design and testing shall reduce the risk of data flow between isolated entities. The following types of data flow shall be considered:

1. **Native data flow** – data of the designed protocol passed between the different TOE interfaces (for example Universal Serial Bus (USB) packets flowing between TOE USB ports).
2. **Timing signaling data flow** - Timing signaling is a method that may be used to signal data between two entities through the use of timing analysis (see note below).
3. **Analog signaling data flow** - Analog signaling is a method that uses abnormal interference inserted into one entity in order to cause a detectable event on another entity.
4. **Power signaling data flow** - Power signaling occurs when a normal or abnormal power supply event or interference applied to one TOE interface causes a detectable event on another TOE interface (e.g., a TOE powered by one USB port (one computer), wherein the TOE power state can be detected at other USB ports (by other computers)).
5. **State signaling data flow** – State signaling flow is a method that uses computers or peripheral device operation states to signal data across the TOE. If, for example, one connected computer enters a standby state and through the TOE another connected computer senses that first computer state change, then there is potentially a covert channel which may be used to transfer (signal) information across the TOE.

Note that timing signaling is an exploit of the TOE functions to transfer digital data through changes in the timing of certain timed events. As the TOE may use low-power microcontrollers, certain events such as interrupt handling may be affected by workload or certain events.

For example, USB keep-alive packets may be generated by the TOE in accordance with a predefined constant timing schedule. If this timing is altered slightly by events occurring at another TOE interface, then there is a risk that this timing change may be detected and used to transfer data between two isolated entities. For example, a delay of 2 milliseconds in the keep-alive may represent “0” and a delay of 5 milliseconds may represent “1”.

[O.COMPUTER_INTERFACE_ISOLATION]

Note: It is recommended that no shared, single-packaged electronic components be allowed between isolated entities (e.g., two isolated entities may not share a single microcontroller).

Since the TOE and its connected computers may have an independent power source or different power management policies, the same level of isolation defined in the dataflow objectives must be maintained at all times while the TOE is powered up or while it is unpowered.

[O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED]

User data such as keyboard entries should be switched (i.e., routed) by the compliant TOE only to the computer selected by the user.

It is critical that the user data from peripheral input devices flow only to the selected computer. A leakage of user data to another computer interface (also known as an echo) may disclose classified user information (e.g., user credentials typed by the user while the TOE is connected to one computer may be sent at a later time to another connected computer). Therefore, the TOE must provide isolation between the data flowing from peripheral devices to the selected computer and any non-selected computer. (See Annex D, Table 1, Flow L).

[O.USER_DATA_ISOLATION]

As the TOE may be reused inside the organization to serve different users / roles at different times, it is critical that no user information be stored in the TOE. Therefore, the TOE shall not retain user data after it is powered off.

It should be noted that user data does not include TOE or peripheral configuration and therefore, such data may remain at the TOE after it is powered off.

[O.NO_USER_DATA_RETENTION]

The TOE shall purge all user keyboard data from TOE computer interfaces following channel switching and before interacting with the new connected computer. This objective assures that when the TOE is switched, user keyboard data does not flow to the previously connected computer.

[O.PURGE_TOE_KB_DATA_WHILE_SWITCHING]

Note that the above objective covers only the keyboard user data in the TOE. It does not cover the data that may be buffered in the keyboard device and therefore it is recommended that the TOE will ignore the first 100 milliseconds of keyboard data coming from the keyboard following channel switching.

As peripheral protocols become more capable, multiple functions may be combined into a single physical interface. The use of such protocols in the TOE shall be avoided as the protection and isolation cannot be assured with such protocols. Protocols such as DisplayPort may be used if the TOE is capable of mitigating and removing content other than video and audio. The use of docking protocols such as DockPort, USB docking, Thunderbolt, etc., is not allowed in the TOE.

Note: Composite protocols such as Mobile High-Definition Link (MHL) 3.0 and higher and USB Type C are allowed in a PSS only if the protocol, as it is used within the TOE, is separated into at least one video only protocol (such as HDMI) and at least one peripheral protocol (such as USB). The TOE may also have an external accessory (for example docking station, cable or dongle) that converts the composite protocol into a standard display and USB interface to enable connection to the TOE computer interface.

[O.NO_DOCKING_PROTOCOLS]

To protect from user data leakages, the TOE shall not allow user data transmission to external entities. Similarly, to protect against data or code injection into the user data transiting the TOE, any data reception from external entities must be disallowed.

Therefore, the TOE may not have any wired or wireless external interfaces to external entities wherein the external entity is any entity except:

a. The TOE evaluated system;
b. The TOE connected computers;
c. The TOE connected peripheral devices; and
d. The TOE power source.

[O.NO_OTHER_EXTERNAL_INTERFACES]

3.2. Audio Devices

It should be noted that the objectives listed in this paragraph are applicable only to a TOE that supports analog audio.

Computer audio may be routed in various ways:

1. Analog audio signals;
2. Digital audio embedded in the video stream or independent digital audio (e.g., Sony/Philips Digital Interface Format, or S/PDIF); and
3. USB audio peripheral devices.

Analog audio requires special attention during TOE design as it may introduce analog leakage concerns. To be compliant with this PP, only analog audio output may be connected to the TOE. This limitation is important in order to prevent exploitation of the connected computer audio codec function used to amplify and detect weak signals inside or around the TOE. Therefore, audio input shared peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE.

[O.NO_ANALOG_AUDIO_INPUT]

USB audio devices (i.e., codecs) are not authorized for use with the TOE. USB audio codecs have configuration memory that may be exploited to enable unauthorized data flows.

Analog audio output in standard computers may be exploited to become audio input in some audio codecs. If one TOE connected computer is hacked and its audio drivers are modified by an attacker, there is a risk that the audio out interface connected to the TOE will become an audio input with very high signal sensitivity. Execution of this attack with connected headphones may result in a remote attacker performing audio eavesdropping in the area of the TOE. Headphones may also be used as low-gain dynamic microphones generating weak analog signals sent back to the TOE. Therefore, the compliant TOE must protect the connected computers from this potential threat. A TOE with an audio switching function shall enforce unidirectional flow of analog signals between the connected computer and the TOE audio peripheral device output. To prevent misuse of headphones as a low-gain dynamic microphone, the TOE shall be designed to assure that reverse audio signal attenuation (signal flowing from the TOE audio device interface to the TOE selected computer audio interface) will be at least 30 dBv measured with 200 mV and 2V input pure sine wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.

[O.UNIDIRECTIONAL_AUDIO_OUT]

Note that the above unidirectional flow attenuation pass criteria is calculated based on the following:

30 dBv = 31.62 signals voltage ratio.

When signal inserted at TOE audio output is 2.00 V peak to peak sine wave, the maximum allowed output measured at the TOE audio computer interface is therefore 63.2mV (or well below noise level).

When a signal inserted at the TOE audio output is a 200 mV peak-to-peak sine wave under a 32 ohm resistive load, the maximum allowed output measured at the TOE audio computer interface is therefore 6.32mV (or well below noise level).

The extended audio frequency range is 1Hz to 50 KHz.

Negative swing is measured when the generated audio signal average voltage is 0V.

The audio dataflow shall be isolated from all other TOE functions. Signal attenuation in the extended audio frequency range between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with a 2V input pure sine wave at the extended audio frequency range, including negative swing signal.

[O.COMPUTER_TO_AUDIO_ISOLATION]

Note that the above port-to-port attenuation pass criterion is calculated based on the following:

45 dBv = 177.82 signals voltage ratio.

When the signal inserted on one TOE computer interface audio input is 2.00 V peak-to-peak sine wave, the maximum allowed output signal voltage measured at another TOE computer interface is therefore 11.2mV (or well below noise level).

The extended audio frequency range is 1Hz to 50 KHz.

Negative swing is measured when the generated audio signal average voltage is 0V.

Digital audio output embedded in the video or independent digital audio output (e.g., S/PDIF) may be switched by the TOE along with the video.

3.3. User Authentication Devices

It should be noted that the objectives listed below are applicable only to a TOE that supports user authentication device.

User authentication devices require a bidirectional channel between the device and the connected computer through the TOE. That channel may contain sensitive user information such as user credentials or user biometric information; therefore, the user authentication function shall be isolated from all other TOE peripheral device functions.

[O.USER_AUTHENTICATION_ISOLATION]

When a user device is being switched from one computer to another by the TOE, there is a risk that data or state information could remain in that device and could be transferred between connected computers. It should be noted that information transferred through non-volatile memory storage on smart-cards or tokens is addressed by other PPs.

Unless the TOE emulates the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device, turning the power off for at least 1 second.

[O.USER_AUTHENTICATION_RESET]

If the TOE emulates the user authentication function (i.e. multiple instances of the user authentication device are coupled to multiple computers at the same time), then once the authentication session is terminated (e.g. the smart card is removed), the session must terminate immediately in all connected computers.

[O.USER_AUTHENTICATION_TERMINATION]

If the TOE is capable of being configured with user authentication device qualification parameters after deployment, then such configuration may only performed by an authenticated administrator.

[O.USER_AUTHENTICATION_ADMIN]

3.4. Control and Monitoring

In order to prevent unintended switching, the TOE shall be designed to require a deliberate user action to switch between connected computers and provide continuous visual indication of the computer to which the user is currently connected.

The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms. Authorized switching mechanisms shall require physical, zero-distance touch and may include push-buttons, touch screen, and mouse or cursor control. Unauthorized switching mechanisms include keyboard shortcuts, also known as “hotkeys,” automatic scanning and voice activation.

[O.AUTHORIZED_SWITCHING]

If the TOE allows more than one authorized switching mechanism, only one method shall be operative at any given time to prevent ambiguous commands.

[O.NO_AMBIGUOUS_CONTROL]

The TOE shall provide continuous visual indication of the computer to which the user is currently connected. Acceptable methods of indication include: Light-Emitting Diode (LED) indicators on the front panel of the TOE, lighted push-buttons, graphic or text displays, and on-screen displays (OSDs). If an OSD is used, it shall be “always on” to ensure that continuous indication is provided. If the TOE is remotely managed, indications shall be replicated at the user location. Critical abnormal user indications such as tampering and failed self-test must also be indicated continuously and replicated at both sides.

[O.CONTINUOUS_INDICATION]

The TOE may enable grouping of peripheral devices (e.g., audio output may be switched separately from the keyboard). Therefore, the compliant TOE shall ensure that the keyboard and mouse devices are always switched together (i.e., they cannot be assigned to different peripheral groups) in order to prevent operational difficulties.

[O.KEYBOARD_AND_MOUSE_TIED]

It should be noted that the objective listed above is applicable only to a TOE that supports keyboard and mouse.

A malicious attack on the TOE may be accelerated if a connected computer is capable of controlling the PSS. Therefore, the TOE shall not allow control through a connected computer.

[O.NO_CONNECTED_COMPUTER_CONTROL]

3.5. Connected Peripheral Devices

3.5.1. General

It is assumed in this PP that all standard peripheral devices may be untrusted; therefore, the TOE shall protect the system from attacks that may exploit such devices to enable unauthorized data flows. Since the TOE may switch peripheral devices of different Shared Peripheral Functions (SPFs) to different computers, data flow between these devices must be protected to prevent unauthorized data flow between connected computers. Therefore, the TOE shall prevent data flow between peripheral devices of different SPFs and the TOE peripheral device ports of different SPFs shall be isolated (See Annex D, Table 1, Flows F and G).

[O.PERIPHERAL_PORTS_ISOLATION]

The TOE shall only allow authorized peripheral device types (See Annex C) for each peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.

[O.DISABLE_UNAUTHORIZED_PERIPHERAL]

3.5.2. Keyboard and Pointing Devices

It should be noted that the objectives listed in this paragraph are applicable only to a TOE that supports keyboard and mouse switching.

The keyboard and pointing device peripheral ports of the TOE shall reject any composite USB devices with endpoints other than those authorized for that specific port (See Annex C). Device rejection shall be accomplished either by completely disabling the connected device or disabling just the unauthorized endpoint(s). Similarly, the TOE shall reject unauthorized peripheral devices or endpoints connected via a USB hub. Alternatively, the TOE may reject all USB hubs.

Note that the TOE may support multiple instances of keyboards and pointing devices. For example, the TOE may support a standard keyboard, a special keypad, a mouse and a multi-touch screen at the same time.

[O.DISABLE_UNAUTHORIZED_ENDPOINTS]

Malicious computers connected to the TOE may exploit certain volatile or non-volatile memory effects in the connected keyboard and pointing device peripherals to temporarily store data. Such temporary data storage may be used to transfer data across connected computers. The use of emulated functions in the compliant TOE is an effective method to protect from such threats. Therefore, the TOE keyboard and pointing device functions shall be:

1. Emulated by the host and device emulators (logically isolated from TOE connected computers – the TOE does not pass keyboard / mouse reports from the user keyboard and mouse to the connected computers) ; and
2. Electrically isolated from TOE computer interfaces (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).

[O.KEYBOARD_MOUSE_EMULATED]

In addition, the TOE keyboard and pointing device data shall be transmitted via a unidirectional flow from the peripheral device to the switched computer. This unidirectional flow enforcement shall be implemented in the TOE through physical (i.e., hardware) methods and not through logical (i.e., firmware dependent) methods (See Annex D, Table 1, Flow B).

[O.KEYBOARD_MOUSE_UNIDIRECTIONAL]

3.5.3. Display Devices

It should be noted that the objectives listed in this paragraph are applicable only to a TOE that supports keyboard and mouse switching.

A TOE that supports Video Graphics Array (VGA), Digital Visual Interface (DVI) or High-Definition Multimedia Interface (HDMI) video shall force native video peripheral data (i.e., red, green, blue, and Transition-Minimized Differential Signaling (TMDS) lines) to follow a unidirectional flow from the switched computer to the connected display device (See Annex D, Table 1, Flow I2).

[O.UNIDIRECTIONAL_VIDEO]

Also, a TOE that supports VGA, DVI, DisplayPort or HDMI video shall force the display EDID peripheral data channel to follow a unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel write transactions initiated by connected computers.

[O.UNIDIRERCTIONAL_EDID]

Lastly, a TOE that supports DisplayPort video shall prevent (i.e., filter or otherwise disable) the following auxiliary channel (AUX) transaction types: EDID write, USB, Ethernet, Audio return channel, universal asynchronous receiver/transmitter (UART) and MCCS. Alternatively, the TOE may prevent the AUX channel from operating at Fast AUX speed (675/720 Mbps) while preventing MCCS transactions.

It should be noted here that this PP relies on VESA DisplayPort revision 1.3. As this standard is still evolving, updating of security objectives may be required to support standard changes in the future.

[O.DISPLAYPORT_AUX_FILTERING]

3.6. Tamper Mitigation

3.6.1. General

In order to mitigate potential tampering and replacement, the TOE shall be devised to ensure that any replacement may be detected, any physical modification is evident, and any logical modification may be prevented.

The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented. This should be accomplished by offering no access to modify the TOE or its memory. To mitigate the risk that a potential attacker will tamper with a TOE and then reprogram it with altered functionality, the compliant TOE external and internal interfaces shall be locked for code read and write. The programmable components of the TOE's programming ports must be permanently disabled for both read and write operations. The TOE's operational code may not be upgradeable through any of the TOE external or internal ports.

[O.NO_TOE_ACCESS]

3.6.2. Tampering Prevention and Detection

The TOE shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the TOE and continue to be available during the TOE deployment.

The TOE shall be labeled with at least one unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain a complete list of manufactured TOE articles and their respective identification markings' unique identifiers.

[O.TAMPER_EVIDENT_LABEL]

If labels are used to satisfy the above objective, then:

1. Labels shall have a vendor-specific design printed over a holographic surface;
2. Labels shall be located in critical locations that are visible to the TOE user in order to enable visual detection of tampering; and
3. Each manufactured TOE shall have a unique set of Tamper Evident Labels. The use of unique serial numbers or codes is required to enable in-service authentication.

It should be noted that the anti-tampering means defined in this PP are not intended to comply with the DoD requirements for AT (for example DOD Directives 5200.39, 5200.44, 8500 Series and 8582.01). The purpose of the basic anti-tampering functionality defined in this PP is to prevent simple attacks from non-sophisticated

The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened.

[O.ANTI_TAMPERING]

The anti-tampering system must have a backup power source to enable tamper detection while the TOE is powered off. A failure or depletion of this backup power source shall trigger the TOE to enter a tamper-evident state.

[O.ANTI_TAMPERING_BACKUP_POWER]

[O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER]

A compliant TOE shall provide clear indication that tampering has been detected.

[O.ANTI_TAMPERING_INDICATION]

Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computer data flows shall be allowed.

[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]

3.7. Self-Testing

In order to detect failures of underlying security mechanisms used by the TOE, the TOE shall perform self-tests following power up or power reset. The self-testing should, at minimum, include testing of:

1. The basic integrity of the TOE hardware and firmware;
2. The basic computer-to-computer isolation (See Annex D, Table 1, Flows J and K); and
3. The other critical security functions (i.e., user control and anti-tampering).

For example, the following steps may be used to test basic isolation during power up:

- The TOE is switched to channel 1;
- A test packet is sent to the computer connected to channel 1; and
- The self-test function checks that all other ports are not receiving any data.

[O.SELF_TEST]

If the TOE fails to pass self-testing,

1. The TOE shall become disabled or the failed components of the TOE shall become disabled; and
2. The TOE shall provide a clear, visible failure indication. Such indication should include details about the detected failure and its severity.

[O.SELF_TEST_FAIL_TOE_DISABLE]

[O.SELF_TEST_FAIL_INDICATION]

4. SECURITY REQUIREMENTS

The Security Functional Requirements (SFRs) included in this section were derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4* with additional extended functional components.

4.1. Conventions

The Common Criteria (CC) defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated by the word "Refinement" in bold text after the element number with additional text in **bold** text and deletions with strikethroughs, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined* text;
- Iteration: Indicated by appending the iteration number in parenthesis (e.g., (1), (2), (3)).
- Text highlighted in blue fonts defines conditions for the following paragraph.

Extended SFRs are identified with the label "_EXT" after the requirement name.

4.2. TOE Security Functional Requirements

4.2.1. Introduction

The Security Functional Requirements (SFRs) are a translation of the security objectives for the TOE. They are usually at a more detailed level of abstraction, but they have to be a complete translation (the security objectives must be completely addressed). The CC requires this translation into a standardized language for several reasons:

- To provide an exact description of what is to be evaluated. As security objectives for the TOE are usually formulated in natural language, translation into a standardized language enforces a more exact description of the functionality of the TOE.
- To allow comparison between two STs. As different ST authors may use different terminology in describing their security objectives, the standardized language enforces using the same terminology and concepts. This allows easy comparison.

This section identifies the SFRs for the TOE. The TOE SFRs that appear below in Table 1 are described in more detail in the following subsections.

SFR	Dependencies	Dependency Satisfied/Rationale
FDP_IFC.1 (1)	FDP_IFF.1 (1)	Yes
FDP_IFF.1 (1)	FDP_IFC.1 (1)	Yes
	FMT_MSA.3	No. The security attributes associated with the Data Isolation Security Function Policy (SFP) are limited to the interface types and data types. The interface type is determined by the type of peripheral device attached to the TOE, and the data type is determined by that interface. These attributes are not subject to security management. Therefore, this SFR and its dependent Security management SFRs, are not appropriate for this TOE type.
FDP_IFC.1 (2)	FDP_IFF.1 (2)	Yes
FDP_IFF.1 (2)	FDP_IFC.1 (2)	Yes
	FMT_MSA.3(1)	No. The security attributes associated with the User Data Protection SFP are limited to the user selected computer interface. The value is user selected and not subject to security management. Therefore, this SFR and its dependent Security management SFRs, are not appropriate for this TOE type.
FDP_ACC.1	FDP_ACF.1	Yes
FDP_ACF.1	FDP_ACC.1	Yes
	FMT_MSA.3(3)	No. The security attributes associated with the peripheral device SFP are limited to the peripheral device type. The value is determined by what has been connected to the TOE, and is not subject to security management. Therefore, this SFR and its dependent Security management SFRs, are not appropriate for this TOE type.
FDP_RIP.1	none	Not applicable
FPT_PHP.1	none	Not applicable
FPT_PHP.3	none	Not applicable
FPT_FLS.1	none	Not applicable

SFR	Dependencies	Dependency Satisfied/Rationale
FPT_TST.1	none	Not applicable
FTA_CIN_EXT.1	none	Not applicable
Optional Requirements (Annex F)		
FAU_GEN.1	none	Not applicable
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	none	Not applicable
FMT_MOF.1	FMT_SMR.1	Yes
	FMT_SMF.1	Yes
FMT_SMF.1	none	Not applicable
FMT_SMR.1	FIA_UID.1	Yes
Selection based Requirements (Annex G)		
FTA_ATH_EXT.1	none	Not applicable
FTA_ATH_EXT.2	none	Not applicable

Table 8: TOE Security Functional Requirements and Dependencies

4.2.2. Class: User Data Protection (FDP)

4.2.3. User Data Information Flow Requirements

FDP_IFC.1(1) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 (1) Simple security attributes

FDP_IFC.1.1(1) The TSF shall enforce the [*User Data Protection SFP*] on
[Subjects: *TOE computer interfaces, TOE peripheral device interfaces*
Information: *User data transiting the TOE*
Operations: *Data flow between subjects*].

Assurance Activity

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

4.2.4. Information flow control functions (FDP_IFF)

FDP_IFF.1(1) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 (1) Subset Information Flow Control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1(1) The TSF shall enforce the [User Data Protection SFP] based on the following types of subject and information security attributes:
[*Subject: TOE computer interfaces*
Subject security attributes: user selected computer interface
Subject: TOE peripheral device interfaces
Subject security attributes: none
Information: User data transiting the TOE
Information security attributes: none].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*The user makes a selection to establish a data flow connection between the* *peripheral device interfaces and one computer interface based on the following rules:*

1. *The attribute User Selected Computer determines the operation Allowed Data Flow such that the only permitted data flows are as listed in the table below:*

Value of User Selected Computer	***Allowed Data Flow***
n	[Selection] *The ST shall include at least one of the following data-flow claims:* *User keyboard peripheral device interface data flowing from peripheral device interface to computer interface #n;* *User mouse peripheral device interface data flowing from peripheral device interface to computer interface #n;* *User display peripheral device interface data flowing from computer interface #1 to one or more user display peripheral device interfaces;* *User authentication peripheral device data flowing bidirectional between computer interface #n and user authentication device peripheral interface; and* *Analog audio output data flowing from computer interface #n to the audio peripheral device interface;*

2. *When the user changes the attribute by selecting a different computer, this causes the TOE to change the data flow accordingly.*
3. *[Conditional] The specific TOE implementation may allow splitting of the user control to different shared peripheral groups. For example, the user authentication device selected computer may be #2, while the keyboard and mouse selected computer device may be #1. In this case, each selection shall be clearly indicated.*
4. *[Conditional] The TOE may support multiple instances of the peripheral devices shown in the table above, or a subset of these peripheral devices.*]

Assurance Activity

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

FDP_IFF.1.3(1) The TSF shall enforce the [the following additional information flow control SFP rules if the TOE supports user authentication devices [Selection]:

1. *If the TOE user authentication device function is not emulated - following an event of the user changing the attribute by selecting a different computer, the TOE must reset the power to the connected user authentication device; or*
2. *If the TOE user authentication device function is emulated - following an event of the user terminating the authentication session while the TOE is switched to computer n, the TOE must immediately terminate any open authentication session in all other connected computers (≠n)*].

Assurance Activity

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

FDP_IFF.1.4(1) The TSF shall explicitly authorize an information flow based on the following rules: [*no additional rules*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules:
[1. The TSF shall deny any information flow between TOE peripheral device interfaces and TOE non-selected computer interfaces.
2. The TSF shall deny any data flow between an external entity and the TOE computer interfaces.
3. The TSF shall deny any user data flow between the TOE and an external entity].

Application Notes:

Note that an external entity is any device that is not part of the evaluated TOE system, its connected computers or connected peripheral devices.

Therefore, with regard to data flow between the TOE and an external entity:

a. TOE status information such as currently selected computer number or firmware version is not user data and therefore may be transmitted to other (external) entities;
b. KVM cables, extenders or adapters connected to a TOE computer interface or to a peripheral interface are not considered external entities and are therefore excluded from this requirement.

Assurance Activity

Assurance Activities for this SFR were integrated with the Data Isolation Requirements SFR below.

4.2.5. Data Isolation Requirements

4.2.6. FDP_IFC.1(2) Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 (2) Simple security attributes

FDP_IFC.1.1(2) The TSF shall enforce the [*Data Isolation SFP*] on
[Subjects: *TOE computer interfaces, TOE peripheral interfaces*
Information: *data transiting the TOE*
Operations: *data flows between computer interfaces*].

Application Notes:

The Data Isolation SFP shall be enforced on data transiting the TOE wherein this data may be:

a. User data – this is typically text typed by the user on the connected keyboard, but may be other types of user information, such as display video; and
b. Other data transiting the TOE – a generalized view of data that may be the result of a hostile action attributable to a threat agent acting from within one or more of the TOE connected computers.

It should be noted that data transiting the TOE does not refer to data generated by the TOE such as TOE monitoring or control information (for example: user selected computer number or name).

Assurance Activity

Assurance Activities for this SFR are in paragraph 4.2.2.6 below.

In addition to reviewing the information in the TSS, the evaluator shall also review the Isolation Documentation and Assessment as described in Annex J of this PP.

4.2.7. Information flow control functions (FDP_IFF)

FDP_IFF.1(2) Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 (2) Subset Information Flow Control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1(2) The TSF shall enforce the [*Data Isolation SFP*] based on the following types of subject and information security attributes:
[Subject: *TOE interfaces*
Subject security attributes: *Interface types (Allowed TOE interface types are listed in Annex C of this PP. Power source and connected computer interfaces are also applicable interface types.)*
Subject: *TOE peripheral device interfaces*
Subject security attributes: *none*
Information: *data transiting the TOE*
Information security attributes: *data types. (The TSF shall enforce the data isolation SFP on the following data types:*

a. *User keyboard key codes;*

b. *User pointing device commands;*

c. *Video information (User display video data and display management data);*

d. *Audio output data; and*

e. *User authentication device data.)*].

Application Note:

Note that the following TOE interface protocols are specifically prohibited:

a. Microphone audio input;
b. DockPort;
c. USB Docking;
d. Thunderbolt; and
e. Other docking protocols.

Assurance Activity

Assurance Activities for this SFR are in paragraph 4.2.2.6 below.

FDP_IFF.1.2(2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*1. During normal TOE operation, the TSF shall permit only user entered keyboard key codes, and user input mouse commands to flow between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface. No flow is permitted between the selected computer interface and the TOE keyboard and mouse peripheral device interfaces. 2. The TSF shall permit information flow and TSF resources sharing between two TOE user peripheral interfaces of the same Shared Peripheral group. Both functions may share the same interface*].

Application Notes:

A Shared Peripheral group refers to user peripherals that are switched together as a group. For example, the user keyboard and user mouse shall be switched together and are therefore in the same Shared Peripheral group.

Data flow between the keyboard and the mouse peripheral interfaces is allowed (ports can be shared or interchangeable).

Normal TOE operation occurs at any time when the TOE is powered on and it is not:

a. Initializing; or
b. In self-test; or
c. Being configured; or
d. In tampered state; or
e. In self-test failed state.

Assurance Activity

Assurance Activities for this SFR are in paragraph 4.2.2.6 below.

FDP_IFF.1.3(2) The TSF shall enforce the [*No additional rules*].

FDP_IFF.1.4(2) The TSF shall explicitly authorize an information flow based on the following rules: [*No additional rules*].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules:

[*1. The TSF shall deny any information flow between TOE Computer Interfaces, except those allowed by the User Data Flow rules;*

2. [Conditional] If the TOE supports keyboard and mouse - The TSF shall deny data flow other than keyboard entries and mouse reports between the TOE keyboard and mouse peripheral device interfaces and the TOE selected computer interface;

3. [Conditional] If the TOE supports keyboard and mouse - The TSF shall deny power flow between the selected computer interface and TOE keyboard and mouse peripheral device interfaces;

4. [Conditional] If the TOE supports keyboard and mouse - The TSF shall deny information flow from the TOE selected computer interface to the TOE keyboard and mouse peripheral device interface;

5. *[Conditional] If the TOE supports user authentication devices - The TSF shall deny data flow of user authentication device data transiting the TOE to non-selected TOE computer interfaces;*

6. *[Conditional] If the TOE supports user authentication devices - The TSF shall assure that the user authentication device computer interfaces are not shared with any other TOE peripheral function interface (keyboard, mouse etc.);*

7. *The TSF shall deny information flow between two TOE user peripheral interfaces in different Shared Peripheral groups;*

8. *[Conditional] If the TOE supports analog audio - The TSF shall deny analog audio information flow between the TOE selected computer audio interface and the user audio device peripheral interface when a microphone peripheral device is intentionally or unintentionally connected to the TOE audio peripheral device interface;*

9. *[Conditional] If the TOE supports analog audio - The TSF shall enforce unidirectional information flow between the TOE selected computer audio interface and the user audio device peripheral interface. Bidirectional information flow shall be denied;*

10. *[Conditional] If video information transiting the TOE is DisplayPort - The TSF shall deny all AUX Channel information flows other than link negotiation, link training and EDID reading;*

11. *[Conditional] If the TOE supports video - The TSF shall deny any information flow from the TOE display peripheral device interface and the selected computer interface with the exception of EDID information that may be passed once at TOE power up or after recovery from TOE reset;*

12. *[Conditional] If the TOE supports video - The TSF shall deny an information flow between the selected computer display interface and the TOE display peripheral device interface on the EDID channel;*

13. *The TSF shall recognize and enable only those peripherals with an authorized interface type as defined in Annex C of this PP. Information flow to all other peripherals shall be denied; and*

14. *All denied information flows shall also be denied when the TOE's power source is removed*].

Application Notes:

To properly comply with the isolation requirements in this PP, It is recommended that the TOE will be designed with the mouse and keyboard peripheral device interfaces electrically and logically isolated from the connected computer interfaces to reduce the risk of potential exploitation of these devices to transfer data through local data storage or state memory. This level of isolation may be met through various methods, including through USB host and USB device emulation.

Note that the keyboard LEDs may be supported by local TOE indications but not through the keyboard LEDs.

4.2.8. Assurance Activities for User Data Information Flow Requirements and Data Isolation Requirements

TSS

The evaluator shall verify that the TOE Summary Specification (TSS) describes all of the interfaces supported in each port group. Any options to switch peripherals independently from the keyboard and mouse must be described.

The evaluator shall also verify that the TSS lists and describes all TOE control options.

To improve USB data analysis, prior to the following tests, the evaluator shall receive a full list of all USB endpoints used by the TOE, and their specific functions.

The evaluator shall verify that the TSS describes all of the external interfaces supported by the TOE and that there are no external interfaces other than computer interfaces, power interfaces and peripheral device interfaces. Any wireless or wired interface must be fully described with its intended function.

The evaluator shall verify that the TSS describes all of the interfaces supported in each port group.

[Conditional] If the TOE supports keyboard / mouse –

Any options to switch peripherals independently from the keyboard and mouse must be described.

The evaluator shall examine the TSS and verify that for any human interface device that may be switched independently from the keyboard and mouse, there is a description that explains how this interface is isolated from all other device interfaces. The evaluator shall be able to determine from this description that there are no shared components, shared lines or shared power supplies.

[Conditional] If the TOE supports a user authentication device –

The evaluator shall verify that the TSS provides details about supported user authentication devices. TSS shall also indicate whether the user authentication device is emulated by the TOE or switched.

The evaluator shall examine the TSS to verify that it describes how the user authentication data path is isolated from all other data paths. This section must indicate that the data path used by the user authentication device is not shared with other transiting data. This section must also describe how the USB port for the user authentication device is powered separately from other peripheral device functions.

If the TOE includes an integrated user authentication device, the evaluator shall examine the TSS to verify that is describes:

1. How the user authentication data path is isolated from all other data paths;
2. If the user authentication device is emulated by the PSS or not;

3. If the user authentication device is emulated, then the TSS shall include detailed information describing authentication session termination by the user, and describe how this occurs simultaneously in all connected computers.

[Conditional] If the TOE supports DisplayPort video -

The evaluator shall verify that the TSS describes how the TOE video auxiliary channel (AUX) path blocks information flows other than the minimal set required to establish the video link. The description should discuss the method implemented to prevent unauthorized DisplayPort transactions:

- The TOE prevents the DisplayPort AUX channel link from reaching speeds higher than 1 megabits per second (DisplayPort ver 1.2 or higher) while blocking MCCS transactions; or
- The TOE disassembles the DisplayPort AUX channel transactions to block all unauthorized transactions.

Guidance

The evaluator shall verify that the operational guidance provides clear direction for the connection of computers and peripheral devices to the TOE. Any options to switch peripheral devices independently from the keyboard and mouse must be described, including a description of how this switching is indicated on the PSS.

The evaluator shall verify that the operational guidance provides clear direction for the usage and connection of TOE interfaces. General information may be provided for computer, power and peripheral devices. Any wireless or wired interface that receives or transmits data to or from the TOE must be described in sufficient detail to allow the evaluator to determine if there is a risk that these interfaces could be misused to import or export user data.

The evaluator shall examine the user guidance and verify that the guidance provides users with information on how to recognize a device where the anti-tampering functionality has been activated.

The evaluator shall review the following subjects in the user and administrative guidance to verify that there are no processes or settings that may allow any forbidden data flow between objects:

a) Installation options;
b) TOE configurations:
c) TOE firmware options; or
d) Accessories supplied with TOE

The evaluator shall verify that any cables or accessories supplied with the TOE (as described in the guidance) do not support computer interface types in the following prohibited protocols list:

a. Microphone audio input;

b. Line in audio input;

c. DockPort;

d. USB docking;

e. Thunderbolt; or

f. Other docking protocols.

The evaluator shall verify that the supported peripheral devices and protocols match the information in Annex C of this PP.

[Conditional] If the TOE supports keyboard / mouse –

The evaluator shall examine the TOE user guidance to determine if there are any operating modes that allow peripheral devices to be switched independently from the keyboard and mouse. All such operating modes must be covered in the TSS. The evaluator shall examine the TOE guidance and verify that the TOE does not support microphone or audio line input device interfaces. The evaluator shall also examine the TOE guidance and verify that it includes an explicit warning not to use microphone, line input or headset devices with the TOE.

Tests

4.2.9. General Tests Setup Information

1. Since a PSS typically has a large set of switched peripheral devices and connected computers, in order to prevent duplication of test setup and testing effort, several tests were grouped into larger test sets. The selection of the appropriate test set is based on the specific TOE implementation, which is based on the type of peripheral devices being supported.
2. Each port group switch selection must be tested for each device; however, not all port groups must be connected simultaneously. For example, if testing a 16-port device, the evaluator may use four connected computers, but must change the connected ports several times to ensure all computer port group connections and switch selections are tested. Likewise, a single USB protocol analyzer may be used, but must be moved to test each applicable port. Several of the tests are written assuming a 4 port device. Each test must be adapted to accommodate all of the ports on each tested TOE.
3. The tests assume the use of Windows on each connected computer. It is permissible to perform the tests using Linux based connected machines with similar applications installed.
4. The evaluator is expected to prepare an image or bitmap with an easily visible number to be used as a background for each connected computer in order to identify each channel (e.g., a white background with the number 1 may serve as a desktop background for computer #1.)
5. Note that some of the following tests require knowledge of the USB protocol to properly configure and operate a USB protocol analyzer and USB sniffer.

4.2.10. Test 4.1 – User Control

This test is mandatory for all TOEs claiming compliance to this PP.

The following tests assure that the TOE is compliant with the user switching rules. In this test the evaluator shall verify that switching methods supported by the TOE are those permitted by this PP.

SFRs mapped to the following test steps:

- Switching rules: FDP_IFF.1.2(1) Rule 2
- Split selection: FDP_IFF.1.2(1) Rule 3

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Run an instance of a text editor (such as Notepad) on each connected computer to identify which computer is connected to the user keyboard by the TOE.
3. Connect a display to each computer in order to see all computers at the same time.
4. Turn on the TOE.
5. Test each TOE switching method and verify that all methods are authorized methods and that non-authorized methods cannot be enabled by specific TOE configuration. Verify that the TOE does not support a computer port scanning mode.
6. Attempt to switch the mouse/pointing device to more than one computer at once. Verify that the TOE ignores such commands. At all times, the mouse/pointing device may only be connected to a single computer.
   Note: Output peripherals such as display or audio output may be connected simultaneously to more than one computer.
7. Attempt to switch the TOE to a computer interface that does not exist (e.g., the fifth port in a 4-port TOE) [Conditional] or to a computer channel that was previously disabled (if applicable). The TOE shall refuse to switch to such options.
8. [Conditional] If TOE enables computer channel freeze and channel disable - the evaluator shall examine these functions and verify that they operate in accordance with the operational guidance.

4.2.11. Test 4.2 – Keyboard Switching, Data Isolation and Device Qualification Rules

[Conditional] The following test is mandatory for any TOE that supports one or more user keyboards.

Test Setup

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Run USB Protocol analyzer software in each of the connected computers.
3. Connect a display to each computer in order to see all computers at the same time.
4. Turn on the TOE.

Part 1 - Positive and Negative Keyboard Data-flow Rules Testing

The following steps shall be run to verify that the USB keyboard traffic is properly routed to the selected computer (positive data flow rule) and no other USB traffic leaks to the non-selected computers (negative data flow rule).

SFRs mapped to the following test steps:

- Switching rules: FDP_IFF.1.2(1) Rule 2
- Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1a
- Negative switching: FDP_IFF.1.5(1) Rule 1
- Multiple instances: FDP_IFF.1.2(1) Rule 4

5. Select computer #1.
6. Use the USB keyboard to type text into a text editor application running on computer #1.
7. Verify that the TOE sends data from the USB keyboard peripheral device to the switched computer #1 [Allowed Data Flow]. Verify that keyboard entries are visible in USB Protocol analyzer on computer #1.
8. Switch to each connected computer and verify that no text appears in the text editor application on any of the non-selected computers.
9. Continue typing on the keyboard and check each one of the non-selected computers for keyboard traffic. The only traffic visible in the USB Protocol analyzers should be USB keep-alive (NAK transactions).
10. Disconnect and reconnect the TOE interface cables connected to computer #1. Check each one of the non-selected computers for keyboard traffic. Verify that the only traffic visible in the USB Protocol analyzers is USB keep-alive (NAK transactions).
11. Reboot computer #1. Check each one of the non-selected computers for keyboard traffic. The only traffic visible in any of the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).
12. Enter sleep or suspend mode in computer #1. Check each one of the non-selected computers for keyboard traffic. The only traffic visible in any of the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).

13. Exit suspend mode on computer #1 and delete all of the text typed in the Text Editor application.
14. Repeat Steps 3 to 13 with each connected computer selected and each instance of the keyboard supported by the TOE (if applicable).
15. [Conditional] This step is applicable only for a TOE that supports PS/2 keyboards - Repeat steps 3 to 14 with a PS/2 keyboard.

Part 2 - Keyboard Allowed Data Flow and Allowed Devices

In the following steps, the evaluator shall verify that the TOE USB keyboard device port will disable or reject a device that is not a qualified keyboard. The evaluator shall also examine the enumeration of a qualified keyboard behind a USB hub with an unauthorized device connected to another hub downstream port.

SFRs mapped to the following test steps:

- Allowed devices: FDP_IFF.1.5(2) Rule 13
- Allowed data: FDP_IFF.1.5(2) Rule 2

16. Ensure that the USB keyboard is connected. Type on the keyboard and at the same time verify that the selected computer USB protocol analyzer does not show any USB transactions other than link maintenance messages (keep-alive NAK transactions) and keyboard keystroke reports (i.e., key press and key release codes).
17. Connect a USB storage device to the USB keyboard interface (instead of the USB keyboard).
18. At the same time, examine the selected computer USB protocol analyzer to verify that the only captured transactions are USB keep-alive data (NAK transactions).
19. Verify that no new text appears in the selected computer text editor window.
20. Verify that the real-time hardware information console does not display any new USB devices (recognized or not recognized).
21. Disconnect the USB storage device and connect a USB audio device instead. Repeat steps 18 to 20 above.
22. Disconnect the USB audio device.
23. Reconnect the keyboard, this time connecting it through a USB hub. Connect the USB storage device to another downstream port of the USB hub.
24. Repeat steps 18 to 20. The USB storage device should not be visible in the real-time hardware information console. The keyboard may or may not be visible, depending on the TOE specific implementation.

Part 3 - Keyboard Flow Isolation and Unidirectional Rule

The TOE HID data path shall not support USB traffic other than keyboard and pointing device user inputs. Therefore, in this test it is adequate to validate that the TOE keyboard device interface enumerates and supports qualified keyboard and mouse devices, but does not enumerate and support USB devices that are not HIDs.

In the following steps, the evaluator shall test the TOE to verify that it does not allow direct electrical and dataflow linkage between the computer interfaces and the connected keyboard device interfaces. In addition, the evaluator shall verify that the keyboard data flow is unidirectional.

SFRs mapped to the following test steps:

- Unidir data flow: FDP_IFF.1.5(2) Rule 4, FDP_IFF.1.2(2)
- Power isolation: FDP_IFF.1.5(2) Rule 3
- Data types: FDP_IFF.1.5(2) Rule 2, FDP_IFF.1.2(2)
- Power off isolation: FDP_IFF.1.5(2) Rule 14

25. Power up the TOE.
26. Select computer #1.
27. Use a USB keyboard emulation software application (see additional information in Annex I) running on computer #1 to turn the keyboard Num Lock, Caps Lock and Scroll Lock LEDs on and off. LEDs on the keyboard should not illuminate. [This is true if the TOE complies with the PP requirement to prevent computer to peripheral data flow].
28. Power down the TOE.
29. Disconnect the peripheral interface USB cable connected from the TOE to computer #1. Disconnect the user keyboard.
30. Power up the TOE. Switch the TOE to computer #1.
31. Reconnect the keyboard. Check that immediately following the connection, the Num Lock, Caps Lock and Scroll Lock keyboard LEDs are blinking momentarily and then stay off (indicating that keyboard is powered on, although the selected computer is not connected).
32. Turn the TOE off and disconnect the USB keyboard and mouse. Reconnect the computer #1 interface USB cable. Connect the keyboard and mouse directly to computer #1 if necessary.
33. Open a real-time hardware information console on computer #1.
34. Turn on the TOE and check the computer real-time hardware information console for the presence of the USB keyboard and mouse. If the TOE keyboard and mouse appears in the listed devices, skip directly to step 36 as the TOE has successfully passed emulated keyboard/mouse testing [keyboard and mouse are emulated and unidirectional]. If not, continue to step 35 below.
35. Perform simulated USB keyboard traffic testing in accordance with the following steps:
    a. Connect a USB Generator to the TOE keyboard peripheral device interface port.

b. Configure the USB Generator to enumerate as a generic HID keyboard device and then to generate a random stream of keyboard packets.
c. Connect a USB protocol analyzer device (sniffer) between the TOE computer interface and the USB port on computer #1 to capture the keyboard USB traffic between the TOE and computer #1.
d. Turn on the TOE and verify that no packets cross the TOE following the keyboard enumeration, except for keep-alive traffic (NAK transactions). If the TOE has successfully passed this test, then its keyboard path complies with the requirements by enforcing unidirectional data flow and by providing an emulated keyboard function.

Part 4 - TOE Keyboard Interface Properly Disable Unauthorized Peripheral Devices

In the following steps the evaluator shall verify that the TOE keyboard port properly disables unauthorized USB devices. This is verified through a USB protocol Analyzer device (sniffer) connected between the device and the TOE.

SFRs mapped to the following test steps:

- Authorized devices: FDP_IFF.1.5(2) Rule 13
- Device rejection: FDP_ACF.1

36. Configure the TOE and the operational environment in accordance with the operational guidance.
37. Power up the TOE.
38. Connect the following unauthorized devices to the TOE USB keyboard peripheral interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected:
    a. USB audio device;
    b. USB storage device;
    c. USB camera;
    d. USB user authentication device;
    e. USB printer; and
    f. USB Composite Device evaluation board with HID keyboard, Communication Device Class (CDC), and Mass Storage Class (MSC) devices. CDC and MSC shall be rejected.

Device Rejection shall be verified through:

I. The expected TOE user indication in accordance with the user guidance; and
II. An immediate cessation of captured USB traffic following device enumeration.

39. Repeat Step 38 above with a USB hub connected between the USB protocol analyzer and the USB device. The results should be the same.

40. Repeat Step 38 above with the TOE powered off. The USB protocol analyzer device shall show only keep-alive traffic (NAK transactions), or no USB link at all.

Part 5 - Keyboard User Control

[Conditional] the following test steps are not applicable for isolators (which may not support user control).

In the following steps, the evaluator shall use the keyboard in an attempt to perform TOE switching operations that are not authorized.

SFRs mapped to the following test steps:

- No unauthorized keyboard data flow: FDP_IFF.1.5(2) rule 2

41. Attempt to control the TOE computer selection using the following standard keyboard shortcuts (# denotes computer channel number):
    a. Control – Control – # - Enter
    b. Shift-Shift-#
    c. Num Lock – Minus - #
    d. Scroll Lock – Scroll Lock - #
    e. Scroll Lock – Scroll Lock – Function #
    f. Scroll Lock – Scroll Lock – arrow (up or down)
    g. Scroll Lock – Scroll Lock – a - Enter
    h. Control – Shift – Alt - # - Enter
    i. Alt – Control – Shift #

    The TOE shall not respond to such commands by switching channels. (It should be noted that keyboard shortcuts may be used to perform other functions, such as TOE configuration).
42. Attempt to switch the keyboard/s to more than one computer at once. The TOE shall ignore such commands / prevent such options. At all times, the keyboard/s shall only be connected to a single selected computer.
43. [Conditional] If the device allows for peripheral switching independent of the keyboard and mouse - the evaluator must verify that the switching function behaves in accordance with the guidance, and that the device provides a clear indication of the connection for each peripheral. The evaluator must also verify that the keyboard and mouse are always switched together.

Notes:

1. The USB protocol analyzer shall indicate no USB data payloads while the computer is not selected. No USB packets are allowed other than standard USB keep-alive traffic (NAK transactions).
2. The NAK transaction is a standard USB PID 1010B transaction used to indicate that the receiving device cannot accept data or the transmitting device cannot send data.
3. To comply with the USB standard, immediately before or following TOE (not computer) power state change (power off or on), the TOE may send a small number of packets to the connected computer.

4.2.12. Test 4.3 – Mouse Switching, Data Isolation and Device Qualification Rules

[Conditional] The following test is mandatory for a TOE that supports one or more user mouse, or other pointing device.

Test Setup

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Run USB Protocol analyzer software in each of the connected computers.
3. Connect one display per computer in order to see all computers at the same time.
4. Turn on the TOE.

Part 1 - Positive and Negative Mouse Data-flow Rules Testing

The following steps shall verify that the USB mouse traffic is properly routed to the selected computer (positive data flow rule), and no other USB traffic leaks to the non-selected computers (negative data flow rule).

SFRs mapped to the following test steps:

- Switching rules: FDP_IFF.1.2(1) Rule 2
- Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1b
- Negative switching: FDP_IFF.1.5(1) Rule 1
- Multiple instances: FDP_IFF.1.2(1) Rule 4

5. Switch the TOE to each connected computer and using a USB mouse, position the mouse cursor at the center of each display. Switch the TOE to computer #1 and move the cursor to the bottom right corner of the display.

6. Use the USB mouse to move the cursor on computer #1.
7. Switch the TOE to each connected computer and verify that the cursor is still located at the center of the display. Verify that the TOE sends data from the USB mouse peripheral device to the switched computer #1 [Allowed Data Flow]. Verify that mouse movement and button reports are visible in the computer #1 USB Protocol analyzer software.
8. Switch to each connected computer and verify that no cursor movements are indicated on any of the non-selected computers.
9. Continue moving the cursor and check each one of the non-selected computers for mouse traffic. The only traffic visible in the USB Protocol analyzers should be USB keep-alive (NAK transactions).
10. Disconnect and reconnect the computer #1 TOE interface cables. Check each one of the non-selected computers for mouse traffic. The only traffic visible in the USB Protocol analyzers is USB keep-alive traffic (NAK transactions).
11. Reboot computer #1. Check each one of the non-selected computers for mouse traffic. The only traffic visible in all the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).
12. Enter sleep or suspend mode in computer #1. Check each one of the non-selected computers for mouse traffic. The only traffic visible in all the non-selected computer USB Protocol analyzers is USB keep-alive traffic (NAK transactions).
13. Switch back to computer #1.
14. Repeat Steps 3 to 13 with each connected computer selected.
15. [Conditional] This step is applicable only for a TOE that supports a PS/2 mouse - Repeat steps 3 to 14 with a PS/2 mouse.

Part 2 - Mouse Allowed Data Flow and Allowed Devices

In the following steps the evaluator shall verify that the TOE USB mouse device port will disable or reject devices that are not a qualified pointing device. The evaluator shall also test the enumeration of a qualified mouse behind USB hub having an unauthorized device connected to another hub downstream port.

SFRs mapped to the following test steps:

- Allowed devices: FDP_IFF.1.5(2) Rule 13
- Allowed data: FDP_IFF.1.5(2) Rule 2

16. Reconnect the USB mouse. Move the mouse cursor from side to side and at the same time verify that the selected computer USB protocol analyzer does not show any USB transactions other than link maintenance messages (keep-alive NAK transactions) and mouse reports.
17. Connect a USB storage device instead of the USB mouse.

18. At the same time, check the selected computer USB protocol analyzer to verify that the only captured transactions are USB keep-alive traffic (NAK transactions).
19. Verify that the mouse cursor is no longer moving.
20. Verify that the real-time hardware information console does not display any new USB devices (recognized or not recognized).
21. Disconnect the USB storage device and connect a USB audio device instead. Repeat steps 18 to 20 above.
22. Disconnect the USB audio device.
23. Reconnect the mouse, this time through a USB hub. Connect a USB storage device to another downstream port of the USB hub.
24. Repeat steps 18 to 20. The USB storage device should not be visible in the real-time hardware information console. The mouse device may or may not be visible, depending on the TOE specific implementation.

Part 3 - Mouse Flow Isolation and Unidirectional Rule

The TOE HID data path shall not support USB traffic other than keyboard and pointing device user inputs. Therefore, in this test it is adequate to validate that the TOE mouse device interfaces enumerate and support qualified mouse devices, but do not enumerate and support USB devices that are not HIDs.

In the following steps, the evaluator shall test the TOE to verify that it does not allow direct electrical and dataflow linkage between the computer interfaces and the connected mouse device interfaces. In addition, the evaluator shall verify that the mouse data flow is unidirectional.

SFRs mapped to the following test steps:

- Unidir data flow: FDP_IFF.1.5(2) Rule 4, FDP_IFF.1.2(2)
- Power isolation: FDP_IFF.1.5(2) Rule 3
- Data types: FDP_IFF.1.5(2) Rule 2, FDP_IFF.1.2(2)
- Power off isolation: FDP_IFF.1.5(2) Rule 14

25. Power up the TOE.
26. Select computer #1.
27. Use a USB gaming mouse with programmable LEDs and attempt to configure the LEDs using the mouse application running on computer #1. The mouse programmable LEDs should not change state [This demonstrates that the TOE complies with the PP requirement to prevent computer to peripheral data flow].
28. Power down the TOE.
29. Disconnect the peripheral interface USB cable connected to computer #1 from the TOE. Disconnect the user mouse.

30. Power up the TOE. Switch the TOE to computer #1.
31. Reconnect the mouse. Verify that immediately following the connection, the mouse is illuminated (i.e. powered on, although the selected computer is not connected).
32. Turn the TOE off and disconnect the USB keyboard and mouse. Reconnect the computer #1 interface USB cable. Connect the keyboard and mouse directly to computer #1 if necessary.
33. Open a real-time hardware information console on computer #1.
34. Turn on the TOE and check the computer real-time hardware information console for the presence of a USB keyboard and mouse. If the TOE keyboard and mouse appears in the listed devices, skip directly to step 36 as the TOE has successfully passed emulated keyboard/mouse testing [i.e. the keyboard and mouse are emulated and unidirectional]. If not, continue to step 35 below.
35. Perform simulated USB mouse traffic testing in accordance with the following steps:
    a. Connect a USB Generator to the TOE mouse peripheral device interface port.
    b. Configure the USB Generator to enumerate as a generic HID mouse device and then to generate random stream of mouse report packets.
    c. Connect a USB protocol analyzer device (sniffer) between the TOE computer interface and the USB port on computer #1 to capture the mouse USB traffic between the TOE and computer #1.
    d. Turn on the TOE and verify that no packets cross the TOE following mouse enumeration, except for keep-alive traffic (NAK transactions). If TOE has successfully passed this test, then its mouse path complies with the requirements by enforcing unidirectional data flow and by providing an emulated mouse function.

Part 4 - TOE Mouse Interface Properly Disable Unauthorized Peripheral Devices

In the following steps the evaluator shall verify that the TOE mouse port properly disables unauthorized USB devices. This is verified through a USB protocol Analyzer device (sniffer) connected between the device and the TOE.

SFRs mapped to the following test steps:

- Allowed devices: FDP_IFF.1.5(2) Rule 13
- Device rejection: FDP_ACF.1

36. Reconfigure the TOE and the operational environment in accordance with the operational guidance.
37. Power up the TOE.
38. Connect the following unauthorized devices to the TOE USB mouse peripheral interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected:

a. USB audio device;
b. USB storage device;
c. USB camera;
d. USB user authentication device;
e. USB printer; and
f. USB Composite Device evaluation board with HID keyboard, Communication Device Class (CDC), and Mass Storage Class (MSC) devices. CDC and MSC devices shall be rejected.

Device rejection shall be verified through:

I. TOE user indication in accordance with the user guidance; and
II. An immediate cessation of captured USB traffic following device enumeration.

39. Repeat Step 38 above with a USB hub connected between the USB protocol analyzer and the USB device. The results should be the same as above.
40. Repeat Step 38 above with the TOE powered off. The USB protocol analyzer device shall show only keep-alive traffic (NAK transactions) or no USB link at all.

Part 5 - Mouse User Control

In the following steps the evaluator shall use the mouse in an attempt to perform TOE switching operations that are not authorized.

SFRs mapped to the following test steps:

- No unauthorized mouse data flow: FDP_IFF.1.5(2) Rule 2

41. Attempt to switch the mouse to more than one computer at once. The TOE shall ignore such commands / prevent such options. At all times, the mouse shall only be connected to a single selected computer.
42. [Conditional] If the device allows for peripheral switching independent of the keyboard and mouse, the evaluator must verify that the switching function behaves in accordance with the guidance, and that the device provides a clear indication of the connection for each peripheral. The evaluator must also verify that the keyboard and mouse are always switched together.
43. [Conditional] If the TOE supports cursor control of selected channels then – The evaluator shall repeat steps 41 to 43 with the cursor control.

Notes:

1. The USB protocol analyzer shall indicate no USB data payloads while the computer is not selected. No USB packets are allowed other than standard USB keep-alive traffic (NAK transactions).
2. The NAK transaction is a standard USB PID 1010B transaction used to indicate that the receiving device cannot accept data or the transmitting device cannot send data.
3. To comply with the USB standard, immediately before or following TOE (not computer) power state change (power off or on), the TOE may send a small number of packets to the connected computer.

4.2.13. Test 4.4 – Display Switching, Data Isolation and Unidirectional Flow Rules

[Conditional] The following test is mandatory for a TOE that supports one or more user displays.

Test Setup

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.

Part 1 - Display Positive and Negative Switching Rules

The following steps evaluate the TOE compliance with the allowed data flow as it is applied to the user display data. This test verifies that the TOE does not transfer display or computer state change data to any non-selected computer.

This test requires the use of an Oscilloscope with a proper set of probes to test the presence of video signals. The type of oscilloscope and probes required depend upon the type and speed of the video interface supported by the TOE. For additional information see Annex I of this PP.

Additionally, in the following steps the evaluator shall verify that the video signal does not leak to other computer interfaces while the TOE is unpowered.

SFRs mapped to the following test steps:

- Switching rules: FDP_IFF.1.2(1) Rule 2
- Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1c
- Negative switching: FDP_IFF.1.5(1) Rule 1
- Multiple instances: FDP_IFF.1.2(1) Rule 4
- Unpowered isolation: FDP_IFF.1.5(2) Rule 14

2. Turn on the TOE.

3. Switch the TOE primary display to computer #1.
4. Observe the primary display to verify that the selected computer is the one that is actually shown.
5. Remove the non-selected computer display interface cables from TOE and connect them, one at a time, to the oscilloscope to verify that no SYNC signal is passed through the TOE:
    a. VGA – single ended probe on pins 13 and then 14;
    b. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - differential probe between pins 10 (+) and 12 (-);
    c. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);
    d. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);
    e. DisplayPort - connect pin 18 to a 3.3V power supply via 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+).
6. Repeat steps 4 to 5 while selecting other TOE connected computers. Verify that no SYNC signal is present.
7. Repeat steps 4 to 6 with the TOE unpowered. Verify that no SYNC signal is present.
8. With the scope connected to the computer #2 video interface signals, disconnect / reconnect the computer #1 video cable. Power up the TOE and select computer #1. Attempt to detect the change in the oscilloscope at each one of the #2 computer interface pins. No changes shall be detected.
9. Repeat step 8 for each one of the other computer interfaces (#3 and 4).
10. Repeat steps 8 and 9, but instead of disconnecting / reconnecting the computer, disconnect and reconnect the display.
11. Repeat steps 8 and 9, but instead of disconnecting / reconnecting the computer, reboot the selected computer.
12. Repeat Steps 2 to 11 with each connected computer.
13. [Conditional] If a secondary (or other additional) display is supported - repeat Steps 3 to 11 with the secondary or other display connected to the TOE.
14. Turn the TOE off by removing power. Verify that no connected display shows any video.
15. Repeat step 5 above to verify that no video signal is present while the TOE is unpowered.
16. Repeat steps 2 to 15 with each type of display supported by the TOE (DVI, HDMI, DisplayPort etc.)

Part 2 - DisplayPort Auxiliary (AUX) Channel Data Handling

[Conditional] This test shall be performed only on a TOE that supports native DisplayPort video.

A TOE that supports DisplayPort through conversion to other video formats through an external cable or dongle should not be tested using these procedures. These procedures are applicable to a TOE that supports DisplayPort video format passed through the switch.

Note that in the following steps only DisplayPort cables shall be used. No conversion from other video protocols is allowed in these tests.

SFRs mapped to the following test steps:

- AUX filtering: FDP_IFF.1.5(2) Rule 10

17. Connect at least one computer with a native DisplayPort video output capable of supporting DisplayPort version 1.2 or higher standard. This computer shall be connected to the TOE computer #1 video input interface.
18. Connect at least one display with native DisplayPort input capable of supporting the DisplayPort version 1.2 or higher standard to the TOE display output.
19. Power up the TOE and select computer #1.
20. Verify that the video image is visible and stable on the user display.
21. Power off the TOE.

In the following steps the evaluator shall verify that the test setup excluding the TOE is capable of supporting the DisplayPort version 1.2 or higher protocol.

22. Disconnect the DisplayPort video cable connecting the display and the TOE and insert a DisplayPort AUX channel analyzer in series. Bypass the TOE and connect the video cable directly to the computer.
23. Change the computer display resolution beyond high definition (HD) (i.e., 1920x1200). Verify that the image is still shown on the display.
24. Verify in the AUX channel analyzer that the AUX channel has switched to version 1.2 or higher.

In the following steps the evaluator shall verify that the test setup including the TOE blocks DisplayPort version 1.2 or higher protocol (675/720 Mbps Fast AUX channel speed).

25. Disconnect the video cable from the computer video output and connect it to the TOE video output. Reconnect the TOE video input on computer #1 to the video output on computer #1.
26. Turn on the TOE and check that there is a stable image shown on the user display.
27. Check the AUX channel analyzer to verify that the link is forced to version 1.1 only. If confirmed, then the test is successfully completed (no further testing required – continue to step 33 below). If version 1.2 or higher is detected, then continue with test steps 28 to 38.

In the following steps the evaluator shall verify that a TOE capable of transferring DisplayPort version 1.2 and higher protocol properly blocks unauthorized transactions.

28. Replace computer #1 with a DisplayPort source device capable of generating version 1.2 or higher traffic.
29. Connect the AUX channel analyzer between the TOE and the display.
30. Program the DisplayPort source device to simulate multiple display interactions. As a minimum, the evaluator shall simulate: HDMI Ethernet Audio Control (HEAC), Ethernet and USB.
31. Verify at the AUX channel analyzer that all transactions except for link negotiation, link training and EDID reading are blocked by the TOE. (These are the minimal set of DisplayPort transaction types required to establish video display link. All other transaction types must be blocked by the TOE).

    Note that detailed information regarding these transactions can be found in VESA DisplayPort standard version 1.3 or higher.
32. Repeat Steps 28 to 31 for each TOE computer video interface.

Part 3 - Video and EDID Channel Unidirectional Rule

In the following steps the evaluator shall validate that the TOE video path is unidirectional from the computer interface to the display interface with the exception of EDID, which may be read from the display once at power up and then may be read by the connected computers. The evaluator shall also verify that the TOE does not pass MCCS transactions to the connected display.

SFRs mapped to the following test steps:

- Unidir flow: FDP_IFF.1.5(2) Rule 12
- EDID once: FDP_IFF.1.5(2) Rule 11
- Unpowered isolation: FDP_IFF.1.5(2) Rule 14

33. Run a MCCS control console on computer #1 (see more information in Annex I of this PP). Bypass the TOE and attempt to control the display brightness to confirm that the setup is operating properly.
34. Reconnect the TOE between the computer and the display.
35. Turn on the TOE and verify that a stable image is shown on the user display.
36. Attempt to control the display brightness from computer #1. This control attempt should fail. Failure of the control indicates that the TOE has effectively filtered the MCCS commands issued by the computer.
37. Switch to the other computers and repeat Step 36 for each TOE video interface.
38. Repeat Steps 36 to 37 with the TOE powered off and verify that the MCCS control attempt fails.
39. Select computer #1 and verify that the display shows video from computer #1 as expected.
40. Turn off the TOE. Disconnect the user display from the TOE.
41. Turn on the TOE. After the TOE has completed the self-test, reconnect the user display to the TOE. The TOE may fail to generate video on the user display (i.e., no EDID is read at the TOE power up). If the display is showing video, then run the EDID reading and parsing software on

computer #1 and check that there is no active EDID (i.e., the computer is using a default generic display or reading older display settings from the registry).

42. Turn off the TOE. Connect the display directly to the video output of computer #1.
43. On computer #1, run the MCCS software and attempt to control the display brightness. The display brightness should be changed. [This is a control test to validate that the setup properly handles MCCS].
44. Disconnect the display from the computer and reconnect to the TOE. Reconnect the video output of computer #1 to the TOE.
45. Turn on the TOE.
46. Select computer #1.
47. Attempt to change the display brightness again using the MCCS software on computer #1. This time the display brightness must stay fixed (i.e., the MCCS commands are blocked by the TOE).
48. Power off the TOE.
49. Repeat Steps 9 to 12 for all other TOE computer video interfaces.
50. Power off the TOE and disconnect the computer #1 video output and the display. Connect the display cable to the TOE computer #1 video interface. Connect the computer #1 video cable to the TOE display interface. This configuration will attempt to force video data through the TOE in the reverse direction. Power up the TOE again.
51. Check that the video is not visible in the display.
52. Remove the display cable from the TOE and connect the oscilloscope to verify that no SYNC signal is passed through the TOE:
    a. VGA – single ended probe on pins 13 and 14;
    b. HDMI – connect pin 19 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - differential probe between pins 10 (+) and 12 (-);
    c. DVI-I – connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - single ended probe on pins 8 and C4. Differential probe between pins 23 (+) and 24 (-);
    d. DVI-D - connect pin 16 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - Differential probe between pins 23 (+) and 24 (-);
    e. DisplayPort - connect pin 18 to a 3.3V power supply via a 100 Ohm resistor to provide HOT PLUG DETECT signal; Check for signals - Differential probe between pins 3 (-) and 1 (+) and between 10 (-) and 12 (+).
53. Repeat steps 50 to 52 with the display and oscilloscope connected to each of the TOE computer interfaces with that computer channel selected on the TOE.
54. Repeat steps 50 to 53 with the TOE powered off (no channel selected).

Part 4 – Authorized Video Interfaces

In the following steps the evaluator shall validate that the TOE video interfaces support only authorized video protocols.

SFRs mapped to the following test steps:

- Authorized interfaces: FDP_IFF.1.5(2) Rule 13

55. Review TOE specification and check that the only video interfaces natively supported are one or more of the following: VGA, DVI, HDMI, and DisplayPort. Note that other protocols may be supported only through the use of special cables, adaptors, docking stations and dongles.
56. Check the TOE external interfaces to verify that the only video interfaces natively supported are one or more of the following: VGA, DVI, HDMI, and DisplayPort.

4.2.14. Test 4.5 –User Authentication Device Switching and Isolation Rules

[Conditional] The following test shall be performed only on a TOE that supports a user authentication device.

Test Setup

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Run USB protocol analyzer software on all connected computers to enable the capture of data on the TOE user authentication device USB interface.
3. Install the user authentication application and driver for the qualified user authentication device being used for testing (for example for the smart card reader and card).
4. Connect a qualified user authentication device to the TOE. Note that the user authentication device shall have a power LED or a DVM connected to its USB power lines (USB contacts #1 and #4).
5. Each connected computer must have its own directly connected display (although the display may be moved during testing to accomplish this). Open a real-time hardware information console window on each computer.

Part 1 - Non- Emulated User Authentication Device Function switching and isolation

[Selection] The following test shall be performed only on TOE devices with user authentication functionality that is not emulated. For TOE devices with emulated user authentication device functionality, skip to step 16 below.

The following steps evaluate the TOE compliance with the allowed data flow as it is applied to the non-emulated user authentication device data. In the following test steps, the approved user authentication device is switched to one selected computer, and the evaluator verifies that all other computers are unable to see any USB traffic. The evaluator shall also turn the TOE power off and verify that the connected user authentication device is inaccessible.

SFRs mapped to the following test steps:

- Switching rules: FDP_IFF.1.2(1) Rule 2
- Positive switching (allow data flow) – not emulated : FDP_IFF.1.3(1) Rule 1
- Negative switching: FDP_IFF.1.5(1) Rule 1
- Multiple instances: FDP_IFF.1.2(1) Rule 4
- Powered off isolation: FDP_IFF.1.5(2) Rule 2

6. Turn on the TOE.
7. Switch the TOE (or the TOE user authentication device, if different) to computer #1. Verify that the user authentication device power LED is illuminated / that the DVM reads 5 VDC. Note: If the DVM or power LED is not fast enough to detect the power dip –an oscilloscope may be used for this test instead.
8. Verify that the real-time hardware information console on computer #1 indicates the presence of the user authentication device.
9. View the display on each of the other computers to verify that the real-time hardware information consoles on these computers do not show the user authentication device.
10. Verify that the USB protocol analyzer software running at all non-selected computers does not detect any USB transaction from the TOE (i.e. the link is off or only NAK transactions are detected).
11. Disconnect and reconnect the selected computer TOE interface cables and attempt to detect USB traffic on any non-selected computer USB protocol analyzer (i.e. the link is off or only NAK transactions are detected).
12. Switch the TOE to computer #2 while observing the authentication device power LED / DVM. Power to the authentication device must be interrupted momentarily immediately after the channel is switched.
13. Repeat Steps 7 to 12 with the authentication device connected to each one of the remaining computers.
14. Switch to the computer with the connected authentication device. Turn the TOE off by removing power. Verify that the user authentication device is no longer visible on any of the connected computers.

15. Check that no USB transactions may be detected on the USB protocol analyzer for each connected computer.

Part 2 - Emulated User Authentication Device

[Selection] The following test shall be performed only on a TOE with user authentication functionality that is emulated.

In the following steps the evaluator shall verify that user authentication on one selected channel does not generate USB transactions on the non-selected connected computers. Also, the evaluator shall establish authentication sessions simultaneously with all connected computers and then terminate the session in one selected computer to verify that all other sessions terminate immediately.

Lastly, the evaluator shall establish an authentication session simultaneously with all connected computers and then power off the TOE to assure that all sessions are terminated immediately.

SFRs mapped to the following test steps:

- Switching rules: FDP_IFF.1.2(1) Rule 2
- Positive switching (allow data flow) – emulated : FDP_IFF.1.3(1) Rule 2
- Negative switching: FDP_IFF.1.5(1) Rule 1
- Multiple instances: FDP_IFF.1.2(1) Rule 4
- Session termination: FTA_ATH_EXT.2

16. Configure the TOE and the operational environment in accordance with the operational guidance.
17. Connect a qualified user authentication device to the TOE / use internal (built-in) authentication device.
18. Each connected computer must have its own directly connected display. Open a real-time hardware information console window on each computer.
19. Run USB protocol analyzer software on each connected computer to enable the capturing of the TOE user authentication device USB interface.
20. Turn on the TOE. Switch the TOE (or the TOE user authentication device, if different) to computer #1. Authenticate using computer #1. At the same time, check that the connected computer USB protocol analyzers, except for selected computer, do not show transactions other than USB keep-alive traffic (NAK transactions).
21. Switch the TOE (or the TOE user authentication device, if different) to computer #2.
22. Authenticate using computer #2. At the same time check that the connected computer USB protocol analyzers, except for selected computer, do not show transactions other than USB keep-alive traffic (NAK transactions).

23. Switch the TOE (or the TOE user authentication device, if different) to computer #3.
24. Authenticate using computer #3. At the same time check that the connected computer USB protocol analyzers except for selected computer do not show any transactions other than USB keep-alive traffic (NAK transactions).
25. Switch the TOE (or the TOE user authentication device, if different) to computer #4.
26. Authenticate using #4. At the same time check that the connected computer USB protocol analyzers except for selected computer do not show any transactions other than USB keep-alive traffic (NAK transactions).
27. Verify that all connected computers are logged-on (user authenticated).
28. Terminate the authentication session (for example – pull out the token or smart-card).
29. Verify that all session at each connected computer terminates immediately.
30. Repeat Steps 20 to 26 (skip steps 28 and 29) then power off the TOE.
31. Verify that the session at each connected computer terminates immediately.

Part 3 - User Authentication Data Isolation Rule

[Conditional] The following test steps shall be performed only on a TOE that does not have a built-in user authentication device. This test is not applicable to a TOE with built-in user authentication functionality (parts 3 and 4 are not applicable).

In the following steps, the evaluator shall verify that the process of user authentication for one selected computer does not generate USB traffic on the other USB interfaces of the same computer. Additionally, the evaluator shall check that the same isolation is maintained when the TOE is powered off.

SFRs mapped to the following test steps:

- Interface isolation: FDP_IFF.1.5(2) Rule 5
- Interface not shared: FDP_IFF.1.5(2) Rule 6
- Powered off isolation: FDP_IFF.1.5(2) Rule 14

32. Disconnect the user authentication device.
33. Verify that the TOE computer interfaces used for the user authentication device are different from the TOE computer interfaces used for keyboard and mouse (i.e., the interfaces shall be isolated, but may use a common ground).
34. Connect a USB protocol analyzer device (sniffer) between the keyboard and mouse computer interface for computer #1 on the TOE and the USB port on computer #1.
35. Run USB protocol analyzer software on each of the remaining computers. The USB protocol analyzer shall monitor the USB port connected to the TOE keyboard and mouse interface and the USB port connected to the TOE user authentication device port.
36. Connect and use a qualified USB user authentication device to authenticate to computer #1.

37. Verify that during this connection, enumeration and authentication processes show no USB traffic other than keep-alive traffic (NAK transactions). Verify that, upon completion of the authentication, the USB sniffer and the USB protocol analyzer software instances show no USB traffic other than keep-alive traffic (NAK transactions) on all other USB interfaces.
38. Repeat steps 34 to 37 for each TOE computer interface.
39. Repeat steps 34 to 38 with the TOE powered off.

Part 4 - User Authentication Device Qualification - FDF

[Conditional] The following test steps shall be performed only on a TOE that supports Fixed Device Filtration (FDF) functionality and does not have a built-in user authentication device. For all other TOE devices, skip to step 42 below.

In the following steps the evaluator shall verify that the TOE properly handles qualified and non-qualified devices connected to the user authentication device port.

SFRs mapped to the following test steps:

- Authorized device: FDP_IFF.1.5(2) Rule 13

40. Power up the TOE.
41. Connect the following unauthorized devices to the TOE user authentication device interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected:
    a. USB audio device;
    b. USB storage device;
    c. USB camera;
    d. USB keyboard;
    e. USB printer; and
    f. USB Composite Device evaluation board with HID keyboard, Communication Device Class (CDC), and Mass Storage Class (MSC) devices. CDC and MSC shall be rejected.

Device Rejection shall be verified through:

I. TOE user indication in accordance with the user guidance; and
II. An immediate cessation of captured USB traffic following device enumeration.

Part 5 - User Authentication Device Qualification - CDF

[Conditional] The following test steps shall be performed only on a TOE that supports Configurable Device Filtration (CDF) function, and does not include a built-in user authentication.

In the following steps the evaluator shall verify that the TOE properly handles qualified and non-qualified devices connected to the user authentication device port after proper configuration.

SFRs mapped to the following test steps:

- Authorized device: FDP_IFF.1.5(2) Rule 13
- CDF management: FMT_SMF.1.1 b
- Restrict to admin: FMT_MOF.1.1
- Admin authentication: FIA_UAU.2
- Auditable log: FIA_UID.2.1

42. Power up the TOE.
43. Following the administrative guidance, configure the TOE CDF to accept (white-list) or reject (black-list) USB authentication devices only. Verify that the CDF definitions are only available for logged-on and authenticated administrators.
44. Connect the following devices to the TOE user authentication device interface via a USB protocol analyzer device (sniffer) to verify that the devices are rejected or accepted based on the TOE configuration:
    a. USB user authentication device;
    b. USB audio device;
    c. USB storage device;
    d. USB camera;
    e. USB keyboard; and
    f. USB printer.

Device Rejection shall be verified through:

I. TOE user indication per user guidance; and
II. An immediate cessation of captured USB traffic following device enumeration.

45. Repeat steps 43 to 44 with the USB audio device white-listed.
46. Repeat steps 43 to 44 with the USB storage device white-listed.
47. Repeat steps 43 to 44 with the USB camera device white-listed.
48. Repeat steps 43 to 44 with the USB keyboard device white-listed.
49. Repeat steps 43 to 44 with the USB keyboard device white-listed and the USB camera black-listed.
50. Repeat steps 43 to 44 with the USB printer device white-listed and the USB storage device black-listed.
51. If the TOE CDF supports filtering criteria other than USB device class (for example: sub-class, protocol, vendor ID, device ID) then repeat steps 43 to 44 using at least 4 other criteria.

52. Download or otherwise access the TOE administrative log and verify that the processes performed in steps 42 to 51 are properly recorded.

4.2.15. Test 4.6 – Analog Audio Output Switching, Isolation and data-flow Rule

[Conditional] This test is not required if the device does not support analog audio switching.

> **Warning:** When performing tests with audio, exercise caution when generating loud noises during tests to prevent hearing loss or damage.

The following steps evaluate TOE compliance with the allowed data flow as it is applied to the analog audio output.

Test Setup

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Run media player with different audio files on each of the connected computers.

Part 1 - Positive and Negative Analog Audio Output Switching Rule

In the following steps the evaluator shall confirm that an analog audio signal traversing the TOE from one user-selected connected computer does not leak to the non-selected computers' analog audio interfaces. Similarly, the evaluator shall verify that there is no significant leakage across the non-selected computers.

SFRs mapped to the following test steps:

- Switching rules: FDP_IFF.1.2(1) Rule 2
- Positive switching (allow data flow): FDP_IFF.1.2(1) Rule 1d
- Negative switching: FDP_IFF.1.5(1) Rule 1
- Multiple instances: FDP_IFF.1.2(1) Rule 4

3. Connect amplified speakers to the TOE audio peripheral interface. Set the speakers to approximately 25% volume.
4. Turn on the TOE.

5. On each of the connected computers, play a video movie with a distinctive sound track. A different movie must be used for each connected computer.
6. Switch the TOE (or TOE audio) to computer #1.
7. Listen to the amplified speakers to verify that the movie on computer #1 is the one being played.
8. Repeat Steps 6 to 7 for each connected computer.
9. Turn the TOE off by disconnecting the power. Verify that no audio is heard.
10. Set the speaker volume output on computer #1 to approximately 25% volume level.
11. Connect the amplified speakers to the TOE audio output interface.
12. Run a tone generator program on computer #1. The generator shall be set to the maximum sound level (i.e., volume).
13. Turn on the TOE.
14. Select computer #1.
15. Test the sound controls on computer #1. The following steps may be followed for Windows. Similar steps may be used for Linux based computers:
    a. Open the Windows Control Panel
    b. Select Sound, then the Sounds tab
    c. Select the system sound "Asterisk" and press Test. The Asterisk sound should be heard through the speakers [Allowed Data Flow].
16. Generate an audio tone of 100 hertz (Sine wave) on computer #1. A loud sound should be heard.
17. Connect the amplified speakers plug to the TOE computer interface #2 audio input jack and set the amplified speakers to full volume (100%).
18. Test the sound (e.g., press the Asterisk sound test button) on computer #1 again several times and verify that no sound can be heard through the speakers.
19. Use the sound generator software on computer #1 to generate test tones of 250 and 500 hertz and 1, 2, 4, 8, 10, 12, 14, and 15 kilohertz for a few seconds at each frequency step. Verify that no sound can be heard through the amplified speakers.
20. Repeat Steps 17 to 19 for all other TOE non-selected computer interface audio input ports.
21. Replace the amplified speakers with an oscilloscope and set to measure the peak-to-peak voltage.
22. Replace computer #1 with an external audio signal generator and set to pure sine wave around the average voltage of half output (positive signal only). Set the output signal to 2.00V peak-to-peak. (The oscilloscope may be used to calibrate the signal.)
23. Set the signal generator to generate 1Hz, 1KHz, 4KHz, 8KHz, 12KHz, 20KHz, 30KHz, 40KHz and 60KHz and use the oscilloscope to detect the leaked signal. The detected signal shall be 63.2mV (or well below noise level). This level of signal assures signal attenuation of 30 dBv in the extended audio frequency range.

24. Repeat step 23 with the audio generator set to signal average to 0V (negative swing). The detected signal shall be 63.2mV (or well below noise level). This level of signal assures signal attenuation of 30 dBv in the extended audio frequency range.
25. Repeat step 23 with the output signal set to 200mV peak-to-peak. The detected signal shall be 6.3mV (or well below noise level). This level of signal assures signal attenuation of 30 dBv in the extended audio frequency range.
26. Disconnect the power to the TOE and repeat Steps 15 to 25. The results shall be the same as for the powered on TOE.
27. Power up the TOE again. Select computer #1.
28. To test for audio leakages between two non-selected audio interfaces, plug the computer #1 audio output cable plug into the TOE computer interface #2 audio input jack. Connect the amplified speakers to each of the other TOE audio input jacks. Test the sound (e.g., press the Asterisk sound test button) again several times and verify that no sound can be heard at the amplified speakers.
29. Repeat Step 28 for each one of the remaining non-selected computer interfaces.

Part 2 - Analog Audio Data Flow Rules

In the following steps the evaluator shall verify that the TOE analog audio functions:

a. Are unidirectional (computer interface to peripheral device data flow only);
b. Will reject a microphone if connected to the audio peripheral interface port; and
c. Will attenuate the audio signal from a connected headset to a level that would not enable audio eavesdropping.

Note: For additional information on the required test equipment refer to Annex I of this document.

SFRs mapped to the following test steps:

- Unidir audio: FDP_IFF.1.5(2) Rule 9
- Mic rejection: FDP_IFF.1.5(2) Rule 8
- Enable authorized: FDP_IFF.1.5(2) Rule 13
- Power off isolation: FDP_IFF.1.5(2) Rule 14

30. Connect the amplified speakers to the analog audio output jack on computer #1. (The audio output jack is typically lime green in color.) Set the volume at the speakers to approximately 25%.
31. Connect the TOE interface cable audio plug on computer #1 (i.e., the computer side) to the computer microphone input jack (typically pink in color) instead of the audio output jack.
32. Connect an open 3.5 millimeter stereo plug or jumper cable to the TOE audio peripheral interface jack (see details in Annex I).
33. Power up the TOE and select computer #1.

34. Measure the DC voltage between the ground terminal and each one of the other two terminals (tip and ring) using a digital voltmeter.
35. Verify the voltage is lower than 0.2 volts, assuring that there is no direct current (DC) bias voltage supplied to a microphone.
36. Connect a standard analog PC microphone instead of the open plug to the TOE audio peripheral interface jack.
37. Open the Audio Sound Recorder application on computer #1 and start recording. Speak loudly into the microphone at approximately 1” [25 millimeter] distance.
38. Play the recorded audio track and verify that the sound cannot be heard (i.e., cannot be recognized over background noise). Attempt to hear the right side and left side separately.
39. Connect dynamic headphones (32 ohm typical impedance) instead of the microphone to the TOE audio peripheral interface jack.
40. Repeat Steps 37 to 39 using the standard headphones as a low-gain microphone.
41. Run an audio tone generator program on computer #1 (i.e., sine wave at maximum volume level).
42. Connect the audio output jack computer #1 to the TOE audio peripheral interface jack. This will inject a strong audio signal from computer #1 to the TOE output.
43. Connect the amplified speaker’s audio input plug to the TOE audio interface jack on computer #1 and check that the amplified speaker’s volume is set to approximately 25%.
44. Generate test tones of 250 and 500 hertz and 1, 2, 4, 8, 10, 12, 14, and 15 kilohertz for a few seconds at each frequency step.
45. Verify that the test sound cannot be heard through the amplified speakers.
46. Replace the amplified speakers with an oscilloscope and set to measure peak-to-peak voltage.
47. Replace computer #1 with an external audio signal generator and set to pure sine wave around average voltage 0V (negative swing). Set output signal to 2.00V peak to peak (oscilloscope may be used to calibrate the signal).
48. Set the signal generator to generate 1Hz, 1KHz, 4KHz, 8KHz, 12KHz, 20KHz, 30KHz, 40KHz and 50KHz and use the oscilloscope to detect the leaked signal. The detected signal shall be 11.2mV (or well below noise level). This level of signal assures signal attenuation of 45 dBv in the extended audio frequency range.
49. Turn the TOE off and repeat Steps 41 to 48.

4.2.16. Test 4.7 – No Other External Interfaces

In the following test, the evaluator shall examine the TOE external interfaces to assure that only the interfaces (connectors) allowed by this PP are available.

SFRs mapped to the following test steps:

- No other external devices: FDP_IFF.1.5(1) Rules 2, 3

The evaluator shall:

1. Check the TOE and its supplied cables, and accessories to assure that there are no external wired interfaces other than:
    a. Computer interfaces;
    b. Peripheral device interfaces; and
    c. Power interfaces.
2. Check TSS to verify that the TOE does not support wireless interfaces. Check for radiated emissions data and Radio Frequency certification information.

4.2.17. Test 4.8 – No Flow between Computer Interfaces (USB-to-USB, Power-to-USB)

In this test, the evaluator shall confirm that the following types of events in one TOE computer interface do not have any effect on any other TOE computer interface:

- Computer reboot or power off;
- Normal USB traffic flowing to the selected computer;
- Enumeration of various USB devices on non-selected computer interfaces;
- Peripheral device over-current event effect on non-selected computers; and
- USB power signaling effect between computer interfaces.

SFRs mapped to the following test steps:

- User authentication isolation: FDP_IFF.1.5(1) Rule 1
- General isolation: FDP_IFF.1.5(2) Rule 1
- User authentication isolation: FDP_IFF.1.5(2) Rule 5

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Connect a USB protocol analyzer device (sniffer) between the TOE USB computer interface #2 and computer #2 (i.e., the first non-selected computer).
3. Run USB protocol analyzer software on all remaining computers.
4. Turn on the TOE and observe the TOE enumeration data flow on all USB protocol analyzers.
5. Ensure the TOE is switched to computer #1.
6. Reboot computer #1. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).
7. Generate a high level of USB HID traffic by moving the mouse at high speed and holding down the keyboard space key at the same time. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).
8. Connect and disconnect the following additional USB devices to the keyboard, mouse and user authentication device ports (if applicable): USB keyboard, USB mouse, USB storage device, USB Audio device and USB user authentication device. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).
9. Plug a USB overload plug (USB Type-A plug with a 2.5 ohm / 10 watt resistor connected between position 1 and 4) into the keyboard, mouse and user authentication device ports. The evaluator shall check for any new USB traffic on all non-connected computer USB analyzers. No

packets should be captured other than USB keep-alive traffic (NAK transactions). Remove the plug after the test is completed.

10. Connect a switchable 5 volt power supply with a USB Type-B plug into the TOE USB keyboard, mouse and user authentication device computer interfaces. Modulate the 5 volt supply (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than periodic USB keep-alive traffic (NAK transactions).
11. Repeat Steps 9 to 10 with each one of the other TOE USB ports.

4.2.18. Test 4.9 – No Flow between Computer Interfaces with TOE Powered Off (USB-to-USB, Power-to-USB)

In this test, the evaluator shall confirm that the following types of events in one computer interface do not have any effect on any other computer interface while the TOE is powered off:

- Computer reboot or power off; and
- USB power signaling effect between computer interfaces.

It should be noted that although the TOE is powered off, some components of the TOE may still be powered from the connected computers.

SFRs mapped to the following test steps:

- General isolation: FDP_IFF.1.5(2) Rule 1
- Unpowered isolation: FDP_IFF.1.5(2) Rule 14

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Connect a USB protocol analyzer device (sniffer) between the TOE USB computer interface #2 and computer #2 (i.e., the first non-selected computer).
3. Run USB protocol analyzer software on each of the remaining computers.
4. Turn on the TOE and observe TOE enumeration data flow on all connected computers.
5. Disconnect the power source to the TOE.
6. Check that the TOE USB computer interfaces are alive by observing the presence of periodic keep-alive traffic (NAK transactions) on all connected computers through the USB protocol analyzer. If the USB interface is alive, continue testing steps 7 and 8 below; if not, no further testing is required.

7. Reboot computer #1. Check for any new USB traffic on all non-connected computer USB analyzers. No packets should be captured other than USB keep-alive traffic (NAK transactions).
8. The evaluator shall connect a switchable 5 volt power supply with a USB Type-B plug (see Annex I of this PP for details) to the TOE USB keyboard, mouse and user authentication device computer interfaces. The 5 volt supply shall be modulated (i.e., cycle on and off) manually at various speeds from approximately one cycle per five seconds to one cycle per second. Check for any new USB traffic on the USB protocol analyzer connected to each non-selected computer. No packets should be captured other than USB keep-alive traffic (NAK transactions).

4.2.19. Test 4.10 – No Flow between Computer Interfaces (Power-/ USB-to-Audio)

[Conditional] This test is not required if the TOE device does not support analog audio switching.

In this test, the evaluator shall verify that power events at one TOE USB computer interface do not affect the analog audio output computer interface of another computer.

SFRs mapped to the following test steps:

- General isolation: FDP_IFF.1.5(2) Rule 1
- Unpowered isolation: FDP_IFF.1.5(2) Rule 14

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Set the speaker volume output on computer #1 to maximum (100%).
3. Connect amplified speakers to the TOE peripheral interface audio output and set to maximum volume.
4. Power up the TOE. Select computer #1.
5. Disconnect and reconnect the USB interface cable on computer #2 several times. Verify that no sound (i.e., clicking or digital noise) can be heard through the amplified speakers. [No USB to audio leakage.]
6. Connect the amplified speakers audio input plug to the computer #2 audio input computer interface.
7. Connect a user authentication device to the TOE (e.g., a smart-card reader). Perform authentication to connected computer #1.
8. Verify that no sound can be heard through the amplified speakers.
9. Repeat Steps 4 to 8 for all other computer interface combinations.
10. Repeat steps 5 to 9 with the TOE powered off.

4.2.20. Test 4.11 – Peripheral to Peripheral Interface Rule

[Conditional] The evaluator shall run this test for any TOE implementation in which the peripheral device interfaces may be switched independently (i.e., the user authentication is switched separately from mouse and keyboard). This test is not required if separate switching is not supported.

[Conditional] This test is only required if the two independently switched peripherals have the same protocol (for example both are USB).

In this test, the evaluator shall verify that the TOE implementation properly isolates the peripheral device interfaces that are not switched together.

Note that the following test assumes that the USB keyboard and mouse combination and the USB user authentication device are independently switched. The test may be modified to support different combinations of peripheral devices with minor changes.

SFRs mapped to the following test steps:

- General isolation: FDP_IFF.1.5(2) Rule 1

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Connect one computer (A) with USB protocol analyzer software to channel #1 of the TOE.
3. Connect another computer (B) with USB protocol analyzer software to channel #2 of the TOE.
4. Connect a qualified USB Authentication device to the TOE.
5. Connect a USB keyboard to the TOE through a USB protocol analyzer device (sniffer).
6. Power up the TOE. Switch the keyboard and mouse to computer A and the user authentication device to computer B.
7. Authenticate to computer B and verify that the USB protocol analyzer running on computer A does not detect any USB transactions other than keep-alive traffic (NAK transactions). Verify that the USB protocol analyzer device (sniffer) does not detect any USB transactions other than keep-alive (NAK transactions).
8. Repeat steps 5 to 7 with a USB mouse instead of a keyboard.
9. Power off the TOE.
10. Remove the USB protocol analyzer device (sniffer) and connect the keyboard and the mouse directly to the TOE.
11. Connect the USB protocol analyzer device (sniffer) between the user authentication device and the TOE.
12. Power up the TOE.

13. Type on the keyboard and move the mouse. At the same time check that the USB protocol analyzer running on computer B does not detect any USB transactions other than keep-alive traffic (NAK transactions). Verify that the USB protocol analyzer device (sniffer) does not detect any USB transactions other than keep-alive traffic (NAK transactions).

4.2.21. Access Control policy (FDP_ACC)

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*peripheral device SFP*] on
[Subjects: *Peripheral devices*
Objects: *Console ports*
Operations: *allow connection, disallow connection*].

Assurance Activity

Note: Assurance Activities for this SFR are covered by the next SFR FDP_ACF.1.1 below.

4.2.22. Access control functions (FDP_ACF)

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control,
FMT_MSA.3 (3) Static attribute initialization.

FDP_ACF.1.1 The TSF shall enforce the [*peripheral device SFP*] to objects based on the following:
[Subjects: *Peripheral devices*
Subject security attributes: *peripheral device type*
Objects: *Console ports*
Object security attributes: *none*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*The TOE shall query the connected peripheral device upon initial connection or upon TOE power up and allow connection for authorized peripheral devices in accordance with the table in Annex C of this PP*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*none.*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:
[*The TOE peripheral device interface (console) port shall reject any peripheral device with unauthorized values*].

Application Notes:

It should be noted that the TOE USB keyboard and USB mouse console ports may be interchangeable or combined into one USB composite device port.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes the allowed devices for each peripheral port type. The description does not need to include brand or model information, but must provide the following information:

a. Whether or not the USB keyboard and USB mouse console ports are interchangeable or may be combined into one port (composite USB device);

b. Whether or not PS/2 keyboard and mouse console ports are supported.

c. What types of authentication devices (e.g., smart card, CAC, token, biometric reader) are supported, how they are identified, and whether or not the TOE enables configurable user authentication device profiling (filtering);

d. What audio out devices types are supported; and

e. What user display interface protocols are supported by the TOE.

If hub and composite devices are permitted, the TSS must describe how the TOE filters endpoints.

[Conditional] If the TOE supports fixed user authentication device filtering (FDF) - then the evaluator shall also verify that the TSS includes a statement indicating that the peripheral device qualification profiles cannot be changed after production.

[Conditional] If the TOE supports configurable user authentication device filtering (CDF) - Verify that the TSS provides information on how the whitelist and blacklist are loaded into the TOE and which users are authorized to load / change these parameters. (Only privileged administrators shall be authorized to perform this activity.)

Guidance

The evaluator shall verify that the user guidance provides instructions for the implementation and use of all implemented connection types, and their limitations. The guidance must describe the visual indications provided to a user when a connected device is rejected.

Test

Tests covering this SFR are tests 4.2 and 4.3 above.

4.2.23. Residual Information Protection (FDP_RIP)

FDP_RIP.1 Subset Residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 **[Refinement]** The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects: [*a TOE computer interface*]:

- *immediately after TOE switch to another selected computer;*
- *and on start-up of the TOE*]

Application Notes:

User data held in any TOE component with non-volatile memory is made unavailable to any TOE computer interface upon the next TOE power on. User keyboard data held in any TOE component is made unavailable to the next connected TOE computer interface when the TOE is switched to a different computer.

The TOE shall have a purge memory or Restore Factory Defaults function accessible to the user to delete all TOE stored configuration and settings.

Assurance Activity

TSS

The TSS shall include a detailed Letter of Volatility. The evaluator shall verify that the TSS Letter of Volatility provides at least the following information:

a. It indicates which TOE components have a non-volatile memory, the non-volatile memory technology, manufacturer and part number and memory size.
b. The type of data that the TOE may store on each one of these components.
c. Whether or not each one of these parts is used to store user data and how this data may remain in the TOE after power down.
d. If the specific component may be independently powered by something other than the TOE (for example – by a connected computer).

The TSS must indicate whether or not the TOE has user data buffers and how these buffers are deleted when the user switches to another computer.

Note that user configuration and TOE settings are not user data and therefore may be stored in the TOE on non-volatile memory components.

Guidance

Check the user or administrative guidance for any limitations regarding transfer of the TOE between different security levels / roles in the organization. Ensure this guidance is consistent with the claims in the Security Target.

Check that the user guidance provides a method to purge TOE memory or to Restore Factory Default settings.

Test

4.2.24. Test 4.12 – Residual Information Protection

SFRs mapped to the following test:

- RIP: FDP_RIP.1

The evaluator shall:

1. Verify that the TSS Letter of Volatility provides assurance that no user data remains in the TOE after power down.

2. Perform the TOE memory purge or Restore Factory Defaults according to the guidance and verify that the TOE enters a desirable secure state.

The following test provides some basic indications that the TOE keyboard stack and buffer are properly deleted upon TOE switching to a different computer:

3. Configure the TOE and the operational environment in accordance with the operational guidance.
4. Run a text editor on computers #1 and #2.
5. Set both computers to the highest keyboard repeat rate.
6. Power up the TOE and select computer #1.
7. Type the letter “A” continuously on the user keyboard (i.e., hold down the “A” button). After a few seconds, release the “A” button and switch to computer #2.
8. Hold down the “B” button.
9. Repeat this process several times and verify that only the letter “A” appears on computer #1 and only the letter “B” appears on computer #2.

4.3. Class: Protection of the TSF (FPT)

4.3.1. Passive Detection of a Physical Attack (FPT_PHP)

FPT_PHP.1 Passive detection of a physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Application Notes:

Assurance Activity

TSS

The evaluator shall verify that the TSS indicates that the TOE provides unambiguous detection of physical tampering. The evaluator shall verify that the TSS provides information that describes how the TOE indicates that it has been tampered with and how these indications cannot be turned on by the TOE user.

Guidance

The evaluator shall verify that the user guidance describes the mechanism by which the TOE provides unambiguous detection of physical tampering and provides the user with instructions for verifying that the TOE has not been tampered with.

Test

The test for this SFR combined with the ant-tampering function testing. See test 4.13 below.

4.3.2. Resistance to Physical Attack

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PHP.3.1 **[Refinement]** The TSF shall resist [a physical attack on the TOE for the purpose of gaining access to the internal components, or to damage the anti-tampering battery] to the [TOE Enclosure] by ~~responding automatically such that the SFRs are always enforced~~ **becoming permanently disabled.**

Application Notes:

'Becoming permanently disabled' is interpreted to mean that all connected peripheral devices shall not function.

The design of the TOE enclosure and anti-tampering functions shall assure that any attempt to open the enclosure enough to allow access to the internal components will activate the anti-tampering function.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes the TOE's reaction to opening the device enclosure, or damaging/exhausting the anti-tampering battery associated with the enclosure.

Guidance

The evaluator shall verify that the user guidance warns the user of the actions that will cause the anti-tampering functionality to disable the device.

Guidance shall also include a clear description of the anti-tampering triggering user indications.

Test

4.3.3. Test 4.13 Tampered TOE is permanently disabled and properly isolated

In the following test the evaluator shall attempt to gain physical access to the TOE internal circuitry (enough access to allow the insertion of tools to tamper with the internal circuitry). The TOE anti-tampering function is expected to trigger, causing an irreversible change to the TOE functionality. The evaluator then shall verify that the anti-tampering triggering provides the expected user indications and also disables the TOE.

TOE disabling means that the user would not be able to use the TOE for any purpose – all peripheral devices and computers are isolated.

Note that it is obvious that if the TOE was physically tampered with, then the attacker may easily circumvent the tamper indication means (for example cut the relevant TOE front panel wires). Nevertheless, the following test verifies that the user would be unable to ignore the TOE tampering indications and resume normal work.

Part 1 – Anti-tampering triggering

In the following steps the evaluator shall trigger the anti-tampering function.

SFRs mapped to the following test:

- Passive detection of physical attack: FPT_PHP.1
- Anti-tampering triggering: FPT_PHP.3.1

The evaluator shall:

1. Attempt to open the PSS enclosure enough to gain access to its internal circuitry. The evaluator shall then verify that the TOE becomes permanently disabled and that the TOE

provides the proper indication that it has been tampered with, in accordance with the user guidance.

2. Verify that at least one tamper evident label was damaged in accordance with the user guidance information.
3. Attempt to turn off the tampering indications through user configuration, panel dimming etc. Verify that the tampering indications are persistent.

Part 2 – Anti-tampering is permanent

In the following test steps the evaluator shall attempt to restore normal TOE operation after TOE anti-tampering has been triggered.

SFRs mapped to the following test:

- Anti-tampering is permanent: FPT_PHP.3.2

4. The evaluator shall perform the memory purge or Restore Factory Defaults procedure in accordance with the user guidance and verify that the TOE remains in a disabled state.
5. The evaluator shall attempt to access the TOE settings to reset the tampering state. The configuration functionality shall be inaccessible, or attempts to recover from the tampered state fail.

Part 3 – Anti-tampering isolation

In the following test steps the evaluator shall validate that the TOE behavior conforms to the data isolation requirements when the device has been tampered with (i.e. the TOE anti-tampering function has been triggered).

SFRs mapped to the following test:

- Anti-tampering isolation: FPT_PHP.3.2

6. Use a TOE sample that was previously tampered with (i.e. the TOE anti-tampering function was triggered).
7. Connect the TOE to computers and peripherals as required and power it up. Verify that the TOE indicates the tampered state in accordance with user guidance.
8. Verify that the following data flows are blocked:
   a. [Conditional] If the TOE supports keyboard switching - verify that the keyboard does not function;

b. [Conditional] If the TOE supports mouse switching - verify that the mouse does not function;
c. [Conditional] If the TOE supports display switching - verify that no video is shown on the user display;
d. [Conditional] If the TOE supports user authentication device switching - verify that the authentication device is not shown on any computer; and
e. [Conditional] If the TOE support analog audio device switching - verify that no audio can be heard;

9. Power off the TOE and repeat step 9.

4.3.4. Failure with Preservation of Secure State (FPT_FLS)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state by disabling the TOE when the following types of failures occur: [*failure of the power on self-test, failure of the anti-tampering function*].

Application Notes:

Disabling the TOE shall provide assurance that, as a minimum, no peripheral device is connected to any computer.

Assurance Activity

Assurance Activities for this SFR were integrated with the TSF Testing Assurance Activities below.

4.3.5. TSF Testing (FPT_TST)

FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 **[Refinement]** The TSF shall run a suite of self-tests that includes as minimum:

- **a.** Test of the basic TOE hardware and firmware integrity; and
- **b.** Test of the basic computer-to-computer isolation; and
- **c.** Test of critical security functions (i.e., user control and anti-tampering).

[during initial startup, [*upon reset button activation*]] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2 The TSF shall provide users with the capability to verify the integrity of [the TSF functionality].

FPT_TST.1.3 The TSF shall provide users with the capability to verify the integrity of [the TSF].

Application Notes:

The TOE shall provide visible user indications in case of Self-test failure.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes the self- tests that are performed on start up or on reset (if a reset function is available). The evaluator shall verify that the self-test covers at least the following:

a) a basic integrity test of the TOE hardware and firmware (for example, memory testing and firmware checksum compare);
b) a test of the computer interfaces' isolation functionality (for example, generating data flow on one port and checking that it is not received on another port);
c) a test of the user interface – in particular tests of the user control mechanism (for example checking that the front panel push-buttons are not jammed); and
d) a test of the anti-tampering mechanism (for example checking that the backup battery is functional).

The evaluator shall verify that the TSS describes how the TOE ensures a shutdown upon a self-test failure or a failed anti-tampering function. If there are instances when a shutdown does not occur (e.g., a failure is deemed non-security relevant), those cases are identified and a rationale is provided explaining why the TOE's ability to enforce its security policies is not affected.

The evaluator shall check the TSS to verify that it describes the TOE behavior in case of self-test failure. The evaluator shall verify that the described TOE behavior includes shutting down the PSS functionality once the failure is detected.

Guidance

The evaluator shall verify that the user guidance:

a. describes how the results of self-tests are indicated to the user;
b. provides the user with a clear indication of how to recognize a failed self-test; and
c. details the appropriate actions to be completed in response to a failed self-test.

The evaluator shall verify that the user / administrative guidance provide adequate information on TOE self-test failures, their causes and their indications.

Test

4.3.6. Test 4.14 Self-Test Pass and Fail

In this test the evaluator shall cause a TOE self-test failure to verify that the TOE responds by disabling normal functions and providing proper user indications.

The evaluator shall also attempt to remove / disconnect the anti-tampering battery to check that the TOE indicates that it has been tampered with.

SFRs mapped to the following test:

- Self-test failure: FPT_FLS.1
- Self-testing: FPT_TST.1

The evaluator shall:

1. Receive from the vendor a specially made TOE sample that was assembled and armed without the top part of the enclosure being assembled or secured. (For example, the TOE may have anti-tampering switches secured in the close position with adhesive tape.)
2. Setup and power up the TOE sample and check that it is operating normally (specifically that it does not indicate that it has been tampered with). The evaluator shall verify that the TOE provides the appropriate indication of a passed self-test in accordance with the user guidance.
3. Power off the TOE.

4. The evaluator shall hold the computer #2 channel select push-button while powering up the TOE. The TOE self-test must recognized a jammed button error and enter a failed TOE state in accordance with the user guidance.
5. Verify that the TOE is disabled and that proper user indications are provided.
6. Power off the TOE and power it on again (this time without the #2 button pressed). The TOE should operate normally after passing the self-test.
7. The evaluator shall temporarily remove or disconnect the TOE anti-tampering battery and return it back / connect it back after a short time (few seconds).
8. Power up the TOE and verify that it indicates that it has been tampered with through the proper tampering state indications.
9. Confirm that the TOE normal functionality is disabled – no keyboard, mouse, display, audio switching etc.
10. Turn the TOE on and off several times and confirm that the results are consistent.

4.3.7. TOE Access (FTA_CIN_EXT)

FTA_CIN_EXT.1 Extended: Continuous Indications

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_CIN_EXT.1.1 The TSF shall display a continuous visual indication of the computer to which the user is currently connected, including on power up, [selection: *on reset*].

Application Notes:

1. "On reset" must be selected if the TOE provides a reset option.

The selection may be omitted if a reset function is not provided by the TOE. A TOE may be PP compliant without providing this option. In this case, the evaluator is not required to perform the tests associated with this option.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes how the switch behaves on power up. The TSS must indicate whether or not the TOE has a reset option and, if so, the TSS shall describe how the switch behaves when this option is exercised.

Guidance

The evaluator shall verify that the user guidance notes which computer port group will be connected on TOE power up or recovery from reset, if this is an option. Where a reset option is available, use of this feature must be described in the user guidance.

Test

4.4. Test 4.15 – Power Up Defaults, Continuous Indications and Single Control

In this test the evaluator shall verify that the TOE power up default settings are consistent with the user guidance. If the TOE defaults are affected by the TOE configuration, then each available configuration shall be tested.

The evaluator shall also check that the TOE provides proper consistent indication of each peripheral device group selected. Indications shall be always on.

SFRs mapped to the following test:

- Continuous indications: FTA_CIN_EXT.1.1
- Power up defaults: FTA_CIN_EXT.1.1

The evaluator shall:

1. Configure the TOE and the operational environment in accordance with the operational guidance.
2. Select a connected computer port group and power down the TOE.
3. Power up the TOE and verify that the expected selected computer is indicated, and that this is the computer that is connected.
4. Repeat steps 2 to 3 for several selected configurations, covering at least each one of the available TOE configurations.
5. Verify that the TOE selected computer indications are always on (i.e., continuous) and fully visible to the TOE user.
6. [Conditional] If the TOE allows peripherals to be connected to different computers (i.e., different SPF) - then verify that each selection has its own selection indication.
7. [Conditional] If TOE panel is equipped with a dimming function – verify that in standard room illumination conditions, indications are visible at minimum brightness settings.

4.5. Security Assurance Requirements

The Security Objectives for the TOE in Section 3 were constructed to address threats identified in Section 2. The Security Functional Requirements (SFRs) in Section 4.2 are a formal instantiation of the Security Objectives. The PP draws from the CC Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

While this section contains the complete set of SARs from the CC, the Assurance Activities to be performed by an evaluator are detailed in this section as well as in Section 4.2.

The general model for evaluating TOEs against STs written to conform to this PP is as follows:

After the ST has been approved for evaluation, the Common Criteria Testing Laboratory (CCTL) will obtain the TOE, supporting IT environment, and the administrative guides for the TOE. The Assurance Activities listed in the PP (which will be refined by the CCTL to be TOE-specific, either within the ST or in a separate document) will then be performed by the CCTL. The results of these activities will be documented and presented (along with the administrative guidance used) for validation.

For each assurance family, “Developer Notes” are provided on the developer action elements to clarify what, if any, additional documentation/activity needs to be provided by the developer. For the content/presentation and evaluator activity elements, additional assurance activities are described as a whole for the family, rather than for each element. Additionally, the assurance activities described in this section are complementary to those specified in Section 4.2.

The TOE SARs, summarized in Table 9, identify the management and evaluative activities required to address the threats identified in Section 2 of this PP.

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative user guidance
Tests	ATE_IND.1	Independent testing - conformance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage

Table 9: TOE Security Assurance Requirements

4.6. Class ADV: Development

The information about the TOE is contained in the guidance documentation available to the end user as well as the TSS portion of the ST. While it is not required that the TOE developer write the TSS, the TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The Assurance Activities contained in Section 4.2 should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

4.6.1. ADV_FSP.1 Basic Functional Specification

The functional specification describes the Target of Evaluation Security Functionality Interfaces (TSFIs). It is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that are not directly invokable by TOE users, there is little point in specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. For this PP, the activities for this family should focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional "functional specification" documentation is necessary to satisfy the assurance activities specified.

The interfaces that need to be evaluated are characterized through the information needed to perform the assurance activities listed, rather than as an independent, abstract list.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

Developer Note: As indicated in the introduction to this section, the functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_ FSP.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ADV_ FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Assurance Activities:

There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in Section 4.2 and other activities described for AGD, and ATE SARs. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided.

4.7. Class AGD: Guidance Documents

The guidance documents will be provided with the developer’s ST. Guidance must include a description of how the authorized user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an authorized user.

Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes

- instructions to successfully install the TOE in that environment;
- instructions to manage the security of the TOE as a product and as a component of the larger operational environment; and
- instructions to provide a protected administrative capability through the use of either TOE capabilities, environmental capabilities, or a combination of the two.

Guidance pertaining to particular security functionality is also provided; specific requirements on such guidance are contained in the assurance activities specified in Section 4.2.

4.7.1. AGD_OPE.1 Operational User Guidance

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Developer Note: Rather than repeat information here, the developer should review the assurance activities for this component to ascertain the specifics of the guidance for which the evaluator will be checking. This will provide the necessary information for the preparation of acceptable guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each privileged user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each privileged user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each privileged user role, the available functions and interfaces, in particular all security parameters under the control of the privileged user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each privileged user role, clearly present each type of security-relevant event relative to the privileged user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each privileged user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activities:

Some of the contents of the operational guidance will be verified by the assurance activities in Section 4.2 and evaluation of the TOE according to the Common Evaluation Methodology (CEM). The following additional information is also required.

The operational guidance shall contain instructions for configuring the TOE environment to support the functions of the TOE. These instructions shall include configuration of the TOE as well as configuration of the connected computers and peripheral devices.

4.7.2. AGD_PRE.1 Preparative Procedures

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE, including its preparative procedures.

Developer Note: As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator *shall apply* the preparative procedures to confirm that the TOE can be prepared securely for operation.

Assurance Activities:

The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses the computer platforms and peripheral devices claimed for the TOE in the ST.

4.8. Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

4.8.1. ATE_IND.1 Independent Testing - Conformance

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operational) documentation provided. The focus of the testing is to confirm that the requirements specified in Section 4.2 are being met, although some additional testing is specified for SARs in Section 4.3. The Assurance Activities identify the additional testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

ATE_IND.1.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E The evaluator *shall test* a subset of the TSF to confirm that the TSF operates as specified.

Assurance Activities:

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the CEM and the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance

Activity, the evaluator must document in the test plan that each applicable testing requirement in the PP is covered.

The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test equipment or tools. For each piece of equipment or tool, an argument (not just an assertion) should be provided that the equipment or tool will not adversely affect the performance of the functionality by the TOE and its platform.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a “fail” and “pass” result (and the supporting details), and not just the “pass” result.

4.9. Class ALC: Life-cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor’s development and configuration management process. This is not meant to diminish the critical role that a developer’s practices play in contributing to the overall trustworthiness of a product; rather, it’s a reflection on the information to be made available for evaluation at this assurance level.

4.9.1. ALC_CMC.1 Labeling of the TOE

This component is targeted at identifying the TOE such that it can be distinguished from other products or versions from the same vendor and can be easily specified when being procured by an end user. The TOE will have additional labeling requirements to meet the demands of FPT_PHP.1.

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

Evaluator action elements:

ALC_CMC.2.1E The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activities:

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Additionally, the evaluator shall verify that the labels required by FPT_PHP.1 are present and intact, as follows:

- The TOE is labeled with at least one unique identifying tamper-evident marking (such as unique serial number) that can be used to authenticate the device.
- Tamper evident labels have been placed in critical locations on the TOE enclosure to assure that any attempt to open the enclosure enough to gain access to its internal components will change at least one label to a tampered state.
- at least one tamper evident label is placed in a location that will be visible to the user operating the TOE.

4.9.2. ALC_CMS.1 TOE CM Coverage

Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance activities are covered by the assurance activities listed for ALC_CMC.1.

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C	The configuration list shall include the following: the TOE itself and the evaluation evidence required by the SARs.
ALC_CMS.2.2C	The configuration list shall uniquely identify the configuration items.
	Evaluator action elements:
ALC_CMS.2.1E	The evaluator *shall confirm* that the information provided meets all requirements for content and presentation of evidence.

Assurance Activities:

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

4.10. Rationale

The rationale tracing the threats to the objectives, assumptions to objectives and the objectives to the requirements is contained in Annex E.

5. CONFORMANCE CLAIMS AND REFERENCES

The Conformance Claim indicates the source of the collection of requirements that is met by a PP or a Security Target (ST) that passes its evaluation. Application notes are provided in the Security Functional Requirements (SFR) and Security Assurance Requirements (SAR) sections to further clarify specific requirements that must be met.

5.1. CC Conformance Claims

This Protection Profile is compliant with the following CC documents:

[CC1] - Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 4, September 2012.

[CC2] - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.

[CC3] - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.

[CEM] - Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

This Protection Profile is CC Part 2 extended and CC Part 3 conformant.

5.2. PP Conformance Claim

This Protection Profile does not claim conformance to any other Protection Profile.

5.3. ST Conformance Requirements

Security Targets that claim conformance to this Protection Profile shall meet a minimum standard of strict conformance as defined by section D.2 of CC Part 1.

Strict-PP conformance means the requirements in the PP are met and that the ST is an instantiation of the PP. In order to be conformant to this PP, a TOE must demonstrate Exact Compliance. Exact Compliance, as subset of Strict Compliance as defined by the CC, is defined as the ST containing all of the requirements in section 4 of this PP, and potentially requirements from Annex F and Annex G of this PP. While iteration is allowed, no additional requirements (from the CC parts 2 or 3) are allowed to be included in the ST. Further, no requirements in section 4 of this PP are allowed to be omitted.

With respect to assurance, it is expected that the ST will contain assurance requirements at least equal to or stronger than what is in the PP, and that all assurance activities stated in the PP will be performed.

5.4. Other Referenced Standards and Documents

5.4.1. Industry Standards

1. VESA DisplayPort (DP) Standard Version 1.3 Dated 17 September 2014. Available for VESA members only.
2. Universal Serial Bus Specification Revision 2.0 dated April 27, 2000.

ANNEX A: GLOSSARY AND ACRONYMS

A.1 Common Criteria Definitions

Term	Meaning
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security target - Implementation-dependent statement of security needs for a specific identified TOE.
TOE	Target of evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance. [CC1]
TSF	TOE security functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.
TSFI	Target of Evaluation Security Functionality Interface
TSS	TOE summary specification - Documentation which provides evaluators with a description of the implementation of SFRs in the TOE.

Table 10: Common Criteria Definitions

A.2 Acronyms

Acronym	Meaning
AUX	DisplayPort Auxiliary Channel
CAC	Common Access Card
CCTL	Common Criteria Test Lab
CDC	Communication Device Class
CODEC	Coder-Decoder
dBv	A measurement of voltages ratio – decibel volt
DC	Direct Current
DP	DisplayPort
DSA	Digital Signature Algorithm
DVI	Digital Visual Interface
EDID	Extended Display Identification Data
FDF	Fixed Device Filtration
FIPS	Federal Information Processing Standards
HD	High Definition
HDMI	High Definition Multimedia Interface
HEAC	HDMI Ethernet Audio Control
HID	Human Interface Device
IP	Internet Protocol
USB Keep-Alive NAK transaction	USB 2.0 standard handshake PID (1010B) – Receiving device cannot accept data or transmitting device cannot send data.
KM	Keyboard, Mouse
KVM	Keyboard, Video and Mouse
LED	Light-Emitting Diode
LoS	Line-of-Sight

MCCS	Monitor Control Command Set
MHL	Mobile High-Definition Link
MSC	Mass Storage Class
mV	millivolt
NSA	National Security Agency
NLFSR	Non-Linear Feedback Shift Register
OSD	On-Screen Display
PC	Personal Computer
PIN	Personal Identification Number
PSS	Peripheral Sharing Switch
PS/2	6-pin Mini-DIN connector used for connecting some keyboards and mice to a PC compatible computer system.
S/PDIF	Sony/Philips Digital Interface Format
SP	Special Publication
SPF	Shared Peripheral Functions
TMDS	Transition-Minimized Differential Signaling
UART	Universal Asynchronous Receiver / Transmitter
USB	Universal Serial Bus
V	Volt
VESA	Video Electronics Standards Association
VGA	Video Graphics Array

Table 11: Acronyms

ANNEX B: BASIC USE CASES

Representative use cases are defined below with guidelines to address various configurations that are covered by this PP.

B.1 Use Case 1 - Single User with PSS and Local Monitoring and Control

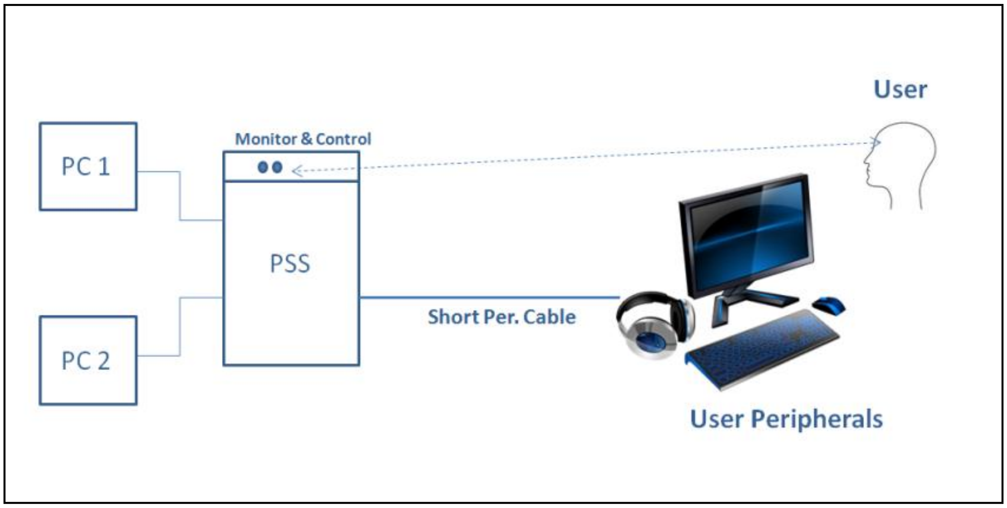


Figure 2: Use Case 1 – Single user with PSS, local monitoring and local control

Notes:

- The user controls the PSS through a user interface located on the PSS (i.e., an internal interface).
- Peripheral devices are connected to the PSS directly with cables (i.e., short cables as opposed to extenders).
- The user shall maintain physical access and full visibility of the PSS monitoring and control functions at all times.

B.2 Use Case 2 - Single User with PSS and Peripheral(s) Connected Directly to Computers

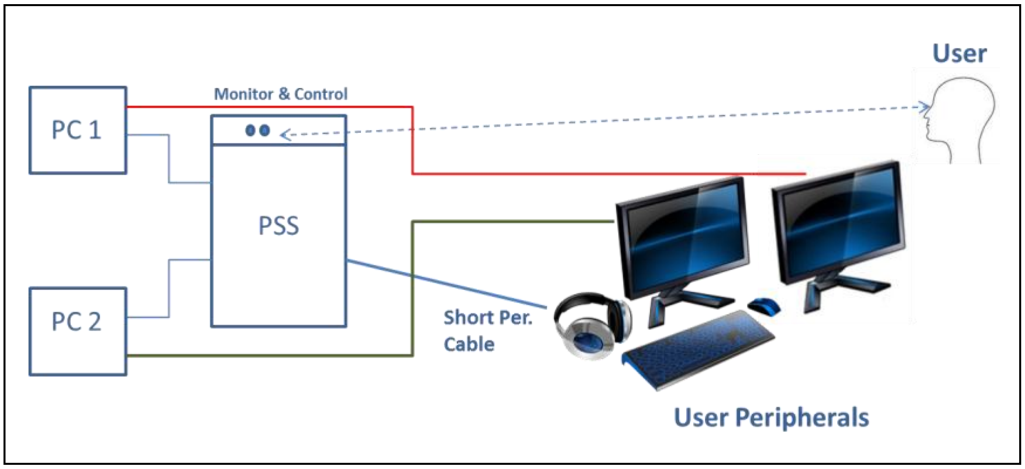


Figure 3: Use Case 2 – Single user with PSS and peripherals connected directly

Notes:

- The PSS switches a subset of the user peripherals. Some peripherals bypass the PSS.
- In this example the user displays are not switched; the PSS is a KM switch (Keyboard, Mouse only). Displays in this example are in the non-switched peripherals group.
- Other peripherals may bypass the switch as long as the keyboard and mouse are at the same peripherals group.

B.3 Use Case 3 - Single User with PSS and Multiple Peripherals of the Same Type

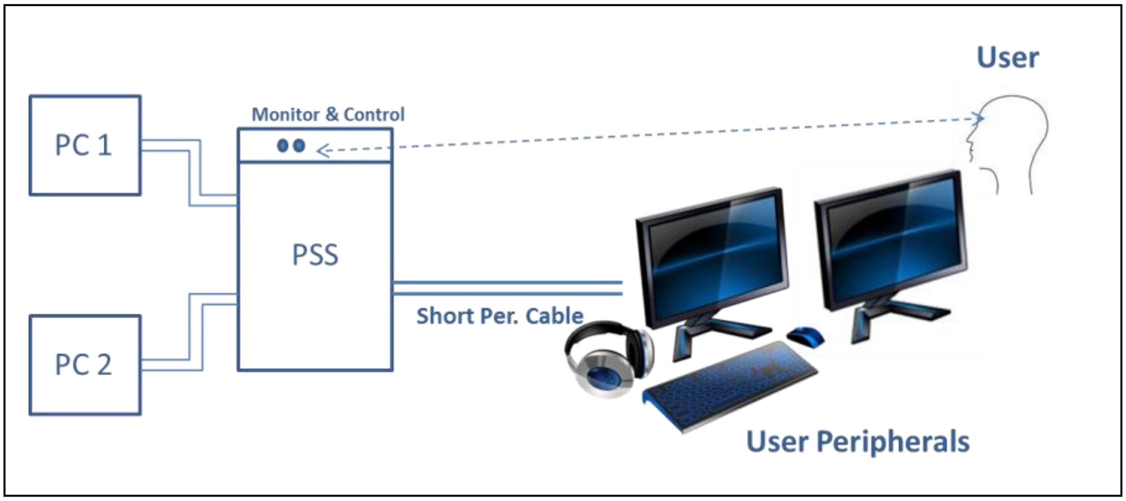


Figure 4: Use Case 3 – Single user with PSS and multiple peripherals of the same type

Notes:

- The PSS has dual displays, both switched synchronously by the PSS (dual-head).
- The PSS supports more than one peripheral from the same type.
- The double lines connecting the computers to the PSS and the PSS to the attached devices represent multiple cables. In this example, they represent two video cables (one for the primary display and one for the secondary display).

B.4 Use Case 4 - Single User with PSS and a Single Computer (Isolator)

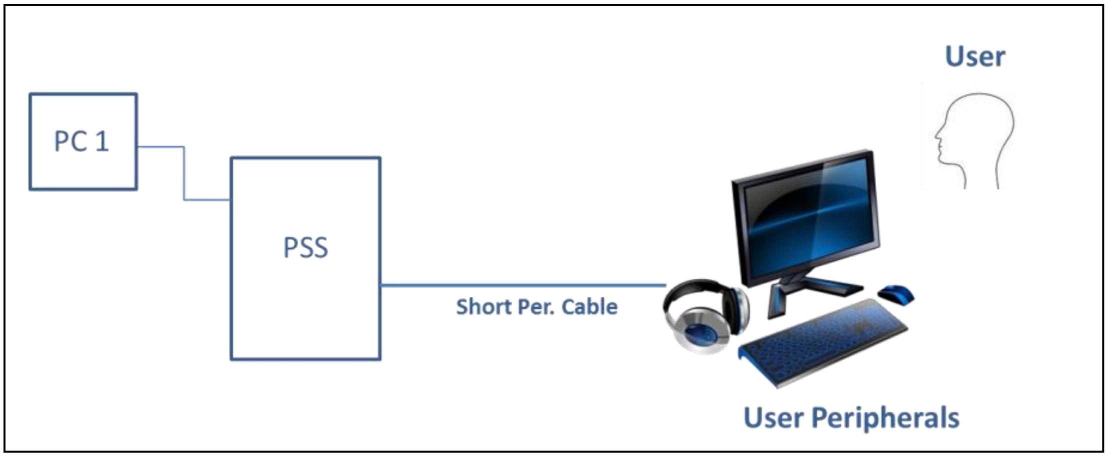


Figure 5: Use Case 4 – Single user with PSS and single computer

Notes:

- The PSS has only one computer connected; therefore, it does not switch computers. Computer may change over time (for example – guest laptop in meeting room),
- The isolator PSS provides mutual isolation and protection between the computer and the user peripherals.

B.5 Use Case 5 - PSS with Single Integrated Video Display (Combiner)

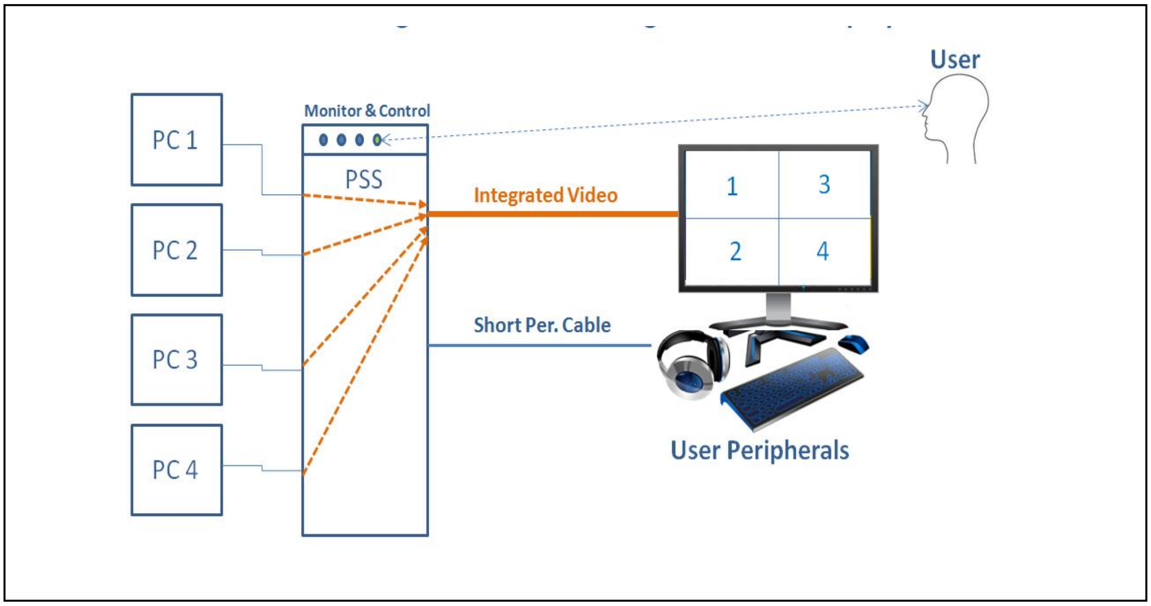


Figure 6: Use Case 5 – PSS with single integrated video display (combiner)

Notes:

- The PSS has one or more displays showing video from one or more computers simultaneously.
- A similar PSS implementation may integrate audio output and a user authentication device from more than one computer.
- The PSS may scale into a video wall to serve multiple users but only one user may interact with the PSS.

B.6 Compliant PSS Guidelines

- Only single user PSSs are supported by this PP (i.e., the PSS may not be shared among users).
- The PSS peripheral devices supported are limited to those listed in Annex C.
- The user may use more than one PSS instance at a time.
- The PSS monitoring and control functions must be local (i.e., built-in or internal).

- The PSS system may have one or more peripheral devices that bypass the PSS (i.e., peripherals are connected directly to a computer).
- The PSS may support one or more instances of same peripheral device.
- The PSS peripheral devices may be divided into one-to-many distinct peripheral groups.
- The PSS may be connected to one-to-many computers.
- The PSS user display may present one-to-many computers’ video output simultaneously.

ANNEX C: AUTHORIZED PERIPHERAL DEVICES AND PROTOCOLS

The following table defines the authorized peripheral device types for each PSS port type. PSS deployment guidelines and/or the PSS internal security functions shall assure that only authorized peripheral devices will be connected to the PSS.

PSS Console Port	Authorized Devices	Authorized Protocols
Keyboard	1. Any wired keyboard and keypad without internal USB hub or composite device functions; 2. KVM extender; 3. USB to PS/2 adapter; and 4. Barcode reader.	1. USB 2. PS/2
Mouse / Pointing device	1. Any wired mouse, or trackball without internal USB hub or composite device functions. 3. Touch-screen; 4. Multi-touch or digitizer; 5. KVM extender.	1. USB 2. PS/2
User authentication device	1. Smartcard, CAC reader; 2. Token; 3. Biometric reader; 4. Any other qualified device if PSS supports configurable user authentication device filtering. 5. PSS internal function listed above.	1. USB
Audio out	1. Analog amplified speakers; 2. Analog headphones; 3. Digital audio appliance.	1. Analog audio output; 2. Digital audio (for example SPDIF); 3. Digital audio embedded inside the video.

Display	1. Display; 2. Projector; 3. Video or KVM extender.	1. VGA; 2. DVI; 3. HDMI; 4. DisplayPort up to version 1.1; 5. DisplayPort higher than version 1.1 with filtration.

Table 12**:** Authorized Devices and Protocols

Notes:

1. USB hub and composite devices are allowed if:
   - The PSS can filter USB endpoints; and
   - At least one endpoint is a keyboard or mouse HID class; and
2. All other endpoints are disabled. Wireless keyboards are not allowed.
3. Wireless mice are not allowed.
4. Keyboard and mouse USB console ports may be interchangeable or specific.
5. PSS User authentication port implementation is selectable between:
   a. Fixed device filtering – TOE shall allow only user authentication devices; or
   b. Configurable device filtering – TOE shall allow any USB device based on configurable rules (for example whitelist and blacklist).
6. User authentication device must be powered by the TOE. External power source is prohibited.
7. The use of analog microphone or line-in audio devices is strictly prohibited.
8. Wireless video transmitters not allowed.

ANNEX D: AUTHORIZED AND UNAUTHORIZED PSS DATA FLOWS

This Annex provides more detailed information regarding the authorized and unauthorized data flows in the PSS. General TOE data flows are outlined first while data flows specific to user authentication devices are outlined separately due to their bidirectional nature.

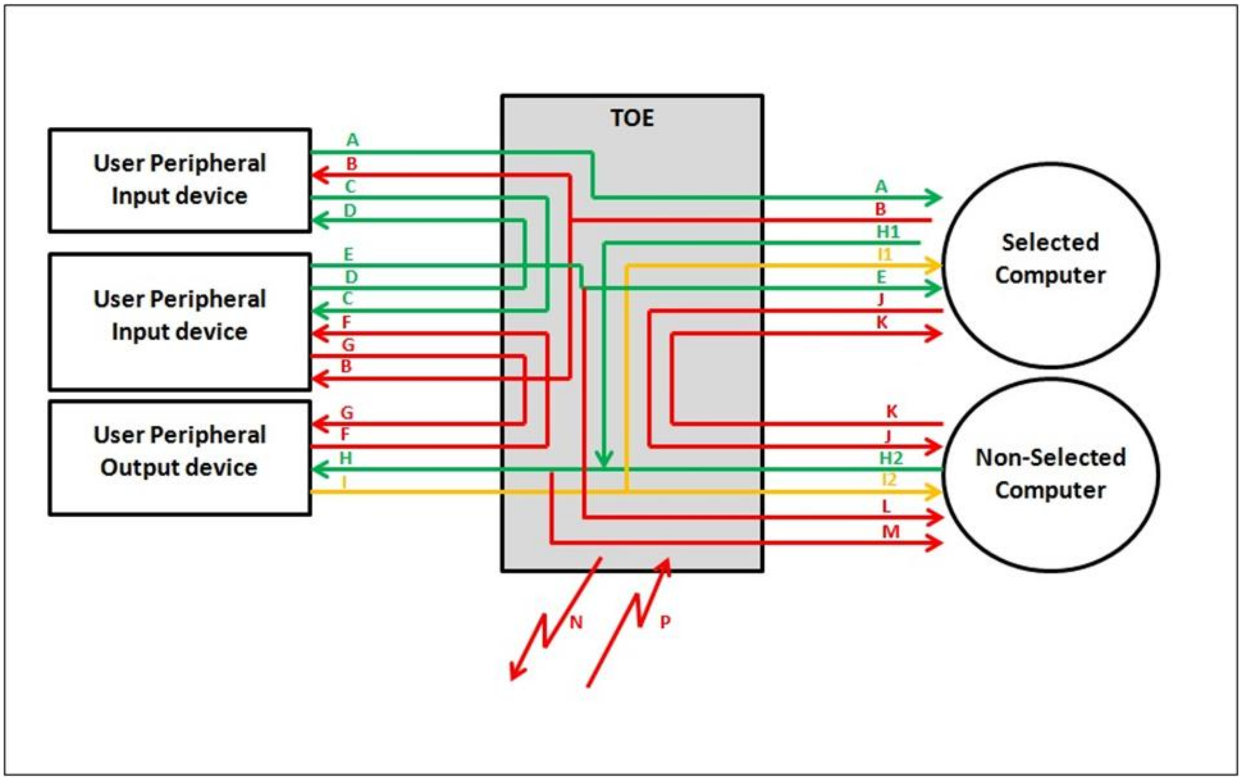

TOE
User Peripheral Input device
A
B
C
D
User Peripheral Input device
E
D
C
F
G
B
User Peripheral Output device
G
F
H
I
A
B
H1
I1
E
J
K
Selected Computer
K
J
H2
I2
L
M
Non-Selected Computer
N
P

Figure 7: Authorized and Unauthorized Data Flows

Flow	From	To	Authorized	Rationale
A, E	User peripheral input device	Selected computer	Yes	Required for normal TOE operation (e.g., keyboard key codes passed to the selected computer).
B	Selected computer	User peripheral input device	No	As peripherals may be untrusted, the data flow through the TOE is allowed only from the peripheral input device to the selected computer to assure that peripherals are not used to leak data.

Flow	From	To	Authorized	Rationale
C, D	User peripheral input device	Another user peripheral input device	Yes	Keyboard and mouse functions may be integrated or endpoints of same USB composite device.
F	User peripheral output device	User peripheral input device	No	May serve as a covert flow channel to leak data from peripheral output to peripheral input device (e.g., H1 -> F -> E will leak data between selected and non-selected computers).
G	User peripheral input device	User peripheral output device	No	May serve as a covert flow channel to leak data from peripheral output to peripheral input device
H	H1 Selected computer H2 Non-selected computer	User peripheral output device	Yes	Display may integrate video output or more than one computer. The user is allowed to see all connected computers' video.
I	User peripheral output device	I1 Selected computer I2 Non-selected computer	OC	Data flow allowed only during TOE boot and limited to EDID data read transactions and link negotiation (in DisplayPort video). All other data transactions such as EDID write, MCCS, asset management, firmware update, USB (DisplayPort video) and Ethernet (DisplayPort video) must be blocked.
J, K	Selected computer; Non-selected computer; Non-selected computer	Non-selected computer; Selected computer; Non-selected computer	No	This is the most critical data flow path for TOE (i.e., leakage between connected computers).
L	User peripheral input device	Non-selected computer	No	User data leakage to a non-selected computer. May be real-time echo or delayed.
M	Selected computer	Non-selected computer	No	Video and audio may not flow to a non-selected computer to prevent potential leakage.

Flow	From	To	Authorized	Rationale
N	Any data flow in TOE	Other entities	No	The TOE should not transmit user data to other external entities (wired or wireless).
P	Other entities	Any data flow in TOE	No	The TOE should not receive user data from other external entities (wired or wireless).
Q	User authentication device	Selected computer	Yes	Bidirectional traffic needed for normal authentication device operation while connected to selected computer.
R	User authentication device data flow in the TOE	Non-selected computer	No	Will leak authentication session information into a non-selected computer.
S	User authentication device	Other peripheral device	No	As peripherals may be untrusted, the user authentication device data flow through the TOE may not be shared with any other peripheral device.
T	Other peripheral device	User authentication device	No	As peripherals may be untrusted, the user authentication device data flow through the TOE may not accept data from any other peripheral device.
U	User authentication device data flow in the TOE	Any other data flow in the TOE	No	User authentication device data flow may have a higher security level compared to all other TOE data flows.

Table 13**:** Authorized and Unauthorized Data Flows

Notes / Definitions:

- User authentication device flows are illustrated in Figure D-3 below.
- OC = On Condition data flow. See applicable restrictions in Table D-1 above.
- User peripheral input device = keyboard or mouse.
- User peripheral output device = display and audio output.
- Selected computer = the computer that the user selected through the TOE.

- Non-selected computer = any computer other than the computer that the user selected through the TOE.

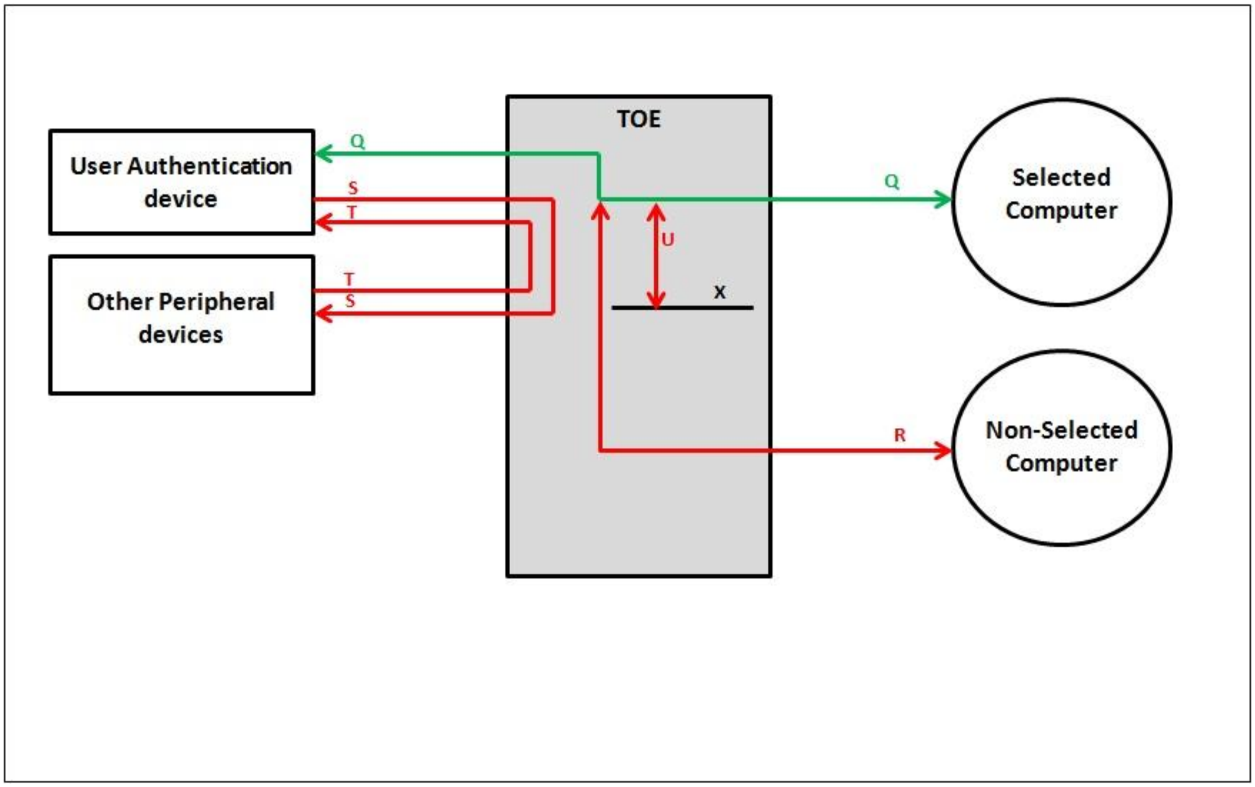


Figure 8: Authorized and Unauthorized User Authentication Device Data Flows

ANNEX E: SUPPORTING TABLES

In this PP, the focus in the initial sections of the document is to use a narrative presentation in an attempt to increase the overall understandability of the threats to PSSs; the methods used to mitigate those threats; and the extent of the mitigation achieved by compliant TOEs. This presentation style does not readily lend itself to a formalized evaluation activity, so this Annex contains the tabular artifacts that can be used for the evaluation activities associated with this document.

E.1 - Assumptions

The specific conditions listed below are assumed to exist in the TOE's Operational Environment. These assumptions reflect the essential environmental conditions on the use of the TOE.

Assumption Name	Assumption Definition
A.NO_TEMPEST	It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.
A.NO_SPECIAL_ANALOG_CAPABILITIES	It is assumed that the computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

Table 14: TOE Assumptions

E.2 - Threats

The following threats are specific to PSSs.

Threat Name	Threat Definition
T.DATA_LEAK	A connection via the PSS between computers may allow unauthorized data flow through the PSS or its connected peripherals.
T.SIGNAL_LEAK	A connection via the PSS between computers may allow unauthorized data flow through bit-by-bit signaling.
T.RESIDUAL_LEAK	A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.
T.UNINTENDED_SWITCHING	A threat in which the user is connected to a computer other than the one to which they intended to be connected.
T.UNAUTHORIZED_DEVICES	The use of an unauthorized peripheral device with a specific PSS peripheral port may allow unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES	The use of an authorized peripheral device with the PSS may still cause unauthorized data flows between connected devices or enable an attack on the PSS or its connected computers. Such threats are possible due to known or unknown device vulnerabilities or due to additional functions within the authorized peripheral device.
T.LOGICAL_TAMPER	An attached device (computer or peripheral) with malware, or otherwise under the control of a malicious user, could modify or overwrite code embedded in the TOE’s volatile or non-volatile memory to allow unauthorized information flows between connected devices.

T.PHYSICAL_TAMPER	A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.
T.REPLACEMENT	A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.
T.FAILED	Detectable failure of a PSS may cause an unauthorized information flow, weakening of PSS security functions, or unintended switching.

Table 15**:** Threats

E.3 - Organizational Security Policies

No specific organization security policies have been identified.

E.4 - Security Objectives for the TOE

TOE Security Objective	TOE Objective Definition
O.COMPUTER_INTERFACE_ISOLATION	The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.
O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED	The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.
O.USER_DATA_ISOLATION	User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected computer and any non-selected computer.
O.NO_USER_DATA_RETENTION	The TOE shall not retain user data after it is powered down.
O.PURGE_TOE_KB_DATA_WHILE_SWITCHING	The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.
O.NO_DOCKING_PROTOCOLS	The use of docking protocols such as DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE.
O.NO_OTHER_EXTERNAL_INTERFACES	The TOE may not have any wired or wireless external interface with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).
O.NO_ANALOG_AUDIO_INPUT	Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE

TOE Security Objective	TOE Objective Definition
O.UNIDIRECTIONAL_AUDIO_OUT	The TOE shall be designed to assure that reverse audio signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sine wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.
O.COMPUTER_TO_AUDIO_ISOLATION	The audio dataflow shall be isolated from all other TOE functions. Signal attenuation between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sine wave at the extended audio frequency range including negative swing signal.
O.USER_AUTHENTICATION_ISOLATION	The user authentication function shall be isolated from all other TOE functions.
O.USER_AUTHENTICATION_RESET	Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.
O.USER_AUTHENTICATION_TERMINATION	If the TOE is emulating the user authentication (instances of the user authentication device are coupled to multiple computers at the same time) then once the authentication session is terminated.
O.USER_AUTHENTICATION_ADMIN	If the TOE is capable of being configured after deployment with user authentication device qualification parameters then such configuration may only performed by an administrator.
O.AUTHORIZED_SWITCHING	The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms.
O.NO_AMBIGUOUS_CONTROL	If the TOE allows more than one authorized switching mechanism, only one method shall be

TOE Security Objective	TOE Objective Definition
	operative at any given time to prevent ambiguous commands.
O.CONTINUOUS_INDICATION	The TOE shall provide continuous visual indication of the computer to which the user is currently connected.
O.KEYBOARD_AND_MOUSE_TIED	The TOE shall ensure that the keyboard and mouse devices are always switched together
O.NO_CONNECTED_COMPUTER_CONTROL	The TOE shall not allow TOE control through a connected computer.
O.PERIPHERAL_PORTS_ISOLATION	The TOE shall prevent data flow between peripheral devices of different SPFs and the TOE peripheral device ports of different SPFs shall be isolated.
O.DISABLE_UNAUTHORIZED_PERIPHERAL	The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.
O.DISABLE_UNAUTHORIZED_ENDPOINTS	The TOE shall reject unauthorized peripheral devices connected via a USB hub. Alternatively, the TOE may reject all USB hubs.
O.KEYBOARD_MOUSE_EMULATED	The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).
O.KEYBOARD_MOUSE_UNIDIRECTIONAL	The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only.
O.UNIDIRECTIONAL_VIDEO	TOEs that support VGA, DVI or HDMI video shall force native video peripheral data (i.e., red, green, blue, and TMDS lines) to unidirectional flow from the switched computer to the connected display device.
O.UNIDIRERCTIONAL_EDID	TOEs that support VGA, DVI, DisplayPort or HDMI video shall force the display EDID peripheral data

TOE Security Objective	TOE Objective Definition
	channel to unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel write transactions initiated by connected computers.
O.DISPLAYPORT_AUX_FILTERING	TOEs that support DisplayPort video shall prevent (i.e., filter or otherwise disable) the following auxiliary channel traffic: EDID write, USB, Ethernet, Audio return channel, UART and MCCS. Alternatively, the TOE may prevent the AUX channel from operating at Fast AUX speed (675/720 Mbps).
O.TAMPER_EVIDENT_LABEL	The TOE shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain a complete list of manufactured TOE articles and their respective identification markings' unique identifiers.
O.ANTI_TAMPERING	The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.
O.ANTI_TAMPERING_BACKUP_POWER	The anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.

TOE Security Objective	**TOE Objective Definition**
O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER	A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.
O.ANTI_TAMPERING_INDICATION	The TOE shall have clear user indications when tampering is detected.
O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE	Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computer data flows shall be allowed.
O.NO_TOE_ACCESS	The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented.
O.SELF_TEST	The TOE shall perform self-tests following power up or powered reset.
O.SELF_TEST_FAIL_TOE_DISABLE	Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.
O.SELF_TEST_FAIL_INDICATION	The TOE shall provide clear and visible user indications in the case of a self-test failure.

Table 16: Security Objectives for the TOE

E.5 - Security Objectives for the Operational Environment

TOE Security Objective	TOE Objective Definition
OE. NO_TEMPEST	The operational environment will not require the use of TEMPEST approved equipment.
OE. NO_SPECIAL_ANALOG_CAPABILITIES	The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.
OE.PHYSICAL	The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.
OE.TRUSTED_ADMIN	The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.

Table 17: Security Objectives for the Operational Environment

E.6 - Security Threats to Security Objectives

The following table contains a mapping of Security Threats to Objectives for the TOE.

Threat	**Objective**	**Rationale**
Cross Computer Flow	Data Flow Isolation	
T.DATA_LEAK A CONNECTION, via the TOE, between connected computers may allow unauthorized data transfer through the TOE or its connected peripherals.	O.COMPUTER_INTERFACE_ISOLATION The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces while TOE is powered.	**O.COMPUTER_INTERFACE_ISOLATION** partially mitigates that threat through the prevention of potential data flows between the different computer interfaces in the TOE. The assurance of isolation between the TOE computer ports prevents data leakages between TOE connected computers directly between the computer interfaces.
	O.COMPUTER_INTERFACE_ISOLATION_UNPOWERED The same level of isolation defined in the dataflow objectives must be maintained at all times, including periods while TOE is unpowered.	**O.COMPUTER_INTERFACE_ISOLATION_UNPOWERED** counters this threat through the prevention of data flow between TOE computer interfaces during periods that the TOE is unpowered. The TOE and its connected computers may have independent power sources or different power management policies. Computer interface isolation in the TOE in the unpowered state must be equal or better than the computer interface isolation in the TOE powered state.
	O.USER_DATA_ISOLATION User data such as keyboard entries should be switched (i.e., routed) by the TOE only to the computer selected by the user. The TOE must provide isolation between the data flowing from the peripheral device to the selected	**O.USER_DATA_ISOLATION** mitigates the threat by ensuring that user data in the TOE will only flow to the user selected computer. To prevent user data leakage, it is critical that user data from the peripheral input device will flow only to the user selected computer. A

Threat	Objective	Rationale
	computer and any non-selected computer.	leakage of user data to another computer interface may disclose classified user information. For example, user credentials typed by the user while the TOE is connected to the secret computer may not leak to any other computer interface to prevent disclosure of classified credentials through another non-classified (and potentially compromised) computer.
	O.NO_DOCKING_PROTOCOLS The use of docking protocols such as DockPort, USB docking, Thunderbolt etc. is not allowed in the TOE. Note: MHL 3.0 and higher or USB Type C is allowed in the TOE only if within the TOE the protocol is separated into one video only protocol (such as HDMI) and one peripheral protocol (such as USB).	**O.NO_DOCKING_PROTOCOLS** mitigates the threat by preventing the use of complex protocols capable of supporting unsecure traffic. As peripheral protocols become more capable, multiple functions may be combined into a single physical interface. The use of such protocols in the TOE shall be limited as the protection and isolation cannot be assured with such protocols when peripheral devices are frequently switched. Such switching may cause data leakages between connected computers through docking protocols. Composite protocols such as DisplayPort, MHL and USB Type C may be used if the TOE is capable of mitigating and effectively removing content other than video and audio.
	O.NO_OTHER_EXTERNAL_INTERFACES The TOE may not have any wired or wireless external interfaces with external entities (external entity is an entity outside the TOE evaluated system, its connected computers	**O.NO_OTHER_EXTERNAL_INTERFACES** counters this threat by ensuring that the TOE would not support external interfaces that may inject code or data into the authorized traffic flowing through it. The presence of a data reception

Threat	Objective	Rationale
	and peripheral devices).	function (wired or wireless) inside the TOE may cause unauthorized data flow or signal leak between external entities and sensitive connected computers and networks.
	O.USER_AUTHENTICATION_ISOLATION The user authentication function shall be isolated from all other TOE functions.	**O.USER_AUTHENTICATION_ISOLATION** mitigates that threat by ensuring that the bidirectional user authentication traffic would not be misused to leak data across the TOE between connected computers. A user authentication device requires a bidirectional channel between the device and the connected computer through the TOE. That channel may contain classified user information. The TOE must prevent leakage of this data to other TOE interfaces.
	O.USER_AUTHENTICATION_RESET Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.	**O.USER_AUTHENTICATION_RESET** mitigates the threat by ensuring that all state and volatile memory in the connected user authentication device will be deleted (through power recycling reset) prior to connecting to a new computer.
	O.PERIPHERAL_PORTS_ISOLATION The TOE shall prevent data flow between peripheral devices of different SPFs. The TOE peripheral device ports of different SPFs shall be isolated (See Annex D, Table 1, Flows F and G).	**O.PERIPHERAL_PORTS_ISOLATION** counters this threat by ensuring that peripheral ports are isolated to prevent unauthorized data flow between peripheral ports. It is assumed in this PP that all standard peripheral devices are untrusted; therefore, the TOE shall protect the system from attacks that may be executed to exploit such devices and enable unauthorized data flows. Since the TOE may switch peripheral devices of different

Threat	Objective	Rationale
		Shared Peripheral Functions (SPFs) to different computers, data flow between these devices must be protected to prevent unauthorized data flow between connected computers.
T.SIGNAL_LEAK A CONNECTION, via the TOE, between COMPUTERS may allow unauthorized data transfer through BIT-BY-BIT signaling.	O.COMPUTER_INTERFACE_ISOLATION The TOE must prevent unauthorized data flow to assure that the TOE and/or its connected peripheral devices would not be exploited in an attempt to leak data. The TOE computer interface shall be isolated from all other TOE computer interfaces.	**O.COMPUTER_INTERFACE_ISOLATION** mitigates the threat by ensuring that the computer interfaces would not be misused to execute a signaling attack. The existence of an unauthorized data flow in the TOE between two computer interfaces may cause signaling leakages across the TOE or its connected peripherals. As computers connected to the TOE may have a wide security gap, this may cause classified data (not necessarily user data) to leak to non-classified (potentially compromised) computers.
	O.NO_OTHER_EXTERNAL_INTERFACES The TOE may not have any wired or wireless external interfaces with external entities (external entity is an entity outside the TOE evaluated system, its connected computers and peripheral devices).	**O.NO_OTHER_EXTERNAL_INTERFACES** mitigates the threat by ensuring that the TOE does not include external interfaces that may inject data into the user data. Such functions may be misused to inject signal data into a connected computer. O.NO_OTHER_EXTERNAL_INTERFACES further mitigates that threat by ensuring that the TOE does not contain any wired or wireless external interface that may export data to outside entity. Such functions may be misused to signal sensitive data from a connected computer.

Threat	Objective	Rationale
	O.NO_ANALOG_AUDIO_INPUT Shared audio input peripheral functions (i.e., analog audio microphone input or line input) are not allowed in the TOE.	**O.NO_ANALOG_AUDIO_INPUT** counters this threat by preventing the passage of the highly-sensitive analog audio input or microphone signals through the TOE. This limitation is important in order to prevent exploitation of the connected computer audio codec function to detect, filter, amplify and detect weak signals inside or around the TOE to perform a signaling attack.
	O.UNIDIRECTIONAL_AUDIO_OUT A TOE with an audio switching function shall enforce unidirectional flow of analog signals between the connected computer and the TOE audio peripheral device output. A TOE with an audio switching function shall be designed to assure that reverse signal attenuation will be at least 30 dBv measured with 200 mV and 2V input pure sine wave at the extended audio frequency range including negative swing signal. The level of the reverse audio signal received by the selected computer shall be minimal to assure that the signal level generated by headphones will be well under the noise floor level.	**O.UNIDIRECTIONAL_AUDIO_OUT** counters this threat by preventing the exploitation of the analog audio output to receive signaled data from a connected computer. Analog audio output in standard computers may be exploited to become audio input in some audio codecs. Audio devices such as headphones may also be used as low-gain dynamic microphones. If the TOE design assures that analog audio reverse signal attenuation is below the noise floor level then the audio signal may not be recovered from the resulted audio stream. This will prevent potential misuse of headphones connected to the TOE for audio eavesdropping. The values selected in the objective were set based on analysis and validated by empirical results.
	O.COMPUTER_TO_AUDIO_ISOLATION The audio data flow shall be isolated from all other TOE functions. Signal attenuation in the	**O.COMPUTER_TO_AUDIO_ISOLATION** counters this threat by assuring that analog audio output converted to input by a malicious driver would not pick up signals from other

Threat	Objective	Rationale
	extended audio frequency range between any TOE computer interface and any TOE audio interface shall be at least 45 dBv measured with 2V input pure sine wave at the extended audio frequency range including negative swing signal.	computer interfaces. A TOE design that assures that audio signals are not leaked to any other TOE interface can effectively prevent a potential signaling leakage across the TOE through the analog audio. The values selected in the objective were set based on analysis and validated by empirical results.
	O.NO_CONNECTED_COMPUTER_CONTROL The TOE shall not allow TOE control through a connected computer.	**O.NO_CONNECTED_COMPUTER_CONTROL** reduces the threat by preventing high speed signaling attacks that misuse TOE channel switching. A malicious signaling attack on the TOE may be accelerated if a compromised connected computer is capable of controlling the TOE selected channel. Bit-by-bit leakages may occur at the rate of one or multiple bits per TOE switch. This rate may increase to several kilobytes per second if the TOE is allowed to be controlled by a connected computer.
	O.USER_AUTHENTICATION_RESET Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.	**O.USER_AUTHENTICATION_RESET** mitigates this threat by eliminating potential state memory in the connected user authentication device after switching to a new computer. Power recycling of the connected user authentication device assures that states and volatile registers will be erased while the TOE switches between computers. Testing has demonstrated that all USB powered authentication devices would reset if powered down for 1 second. In the case that a specific

Threat	Objective	Rationale
		USB device does not properly reset, the vendor may implement longer power down intervals.
T.RESIDUAL_LEAK A PSS may leak (partial, residual, or echo) user data between the intended connected computer and another unintended connected computer. More specifically, a PSS may leak user keyboard entries to a PSS-connected computer other than the selected computer in real-time or at a later time.	O.NO_USER_DATA_RETENTION The TOE shall not retain user data after it is powered down. It should be noted that user data does not include the TOE or peripherals configuration and therefore such data may remain in the TOE after it is powered off.	**O.NO_USER_DATA_RETENTION** counters this threat by preventing user data retention at the TOE when it is being powered off. As a TOE device may be redeployed within the organization to serve different users / roles at different times, it is critical that no user information is stored in the TOE after it is powered off.
	O.PURGE_TOE_KB_DATA_WHILE_SWITCHING The TOE shall purge all user keyboard data from computer interfaces following channel switching and before interacting with the new connected computer.	**O.PURGE_TOE_KB_DATA_WHILE_SWITCHING** assures that when the TOE is switched, user keyboard data will not flow to the previously selected computer. It mitigates this threat by deleting user keyboard data while switching between channels.
Unintended Switching	Control and Monitoring	
T.UNINTENDED_SWITCHING A threat in which the user is connected to a computer other than the one to which they intended to be connected.	O.AUTHORIZED_SWITCHING The TOE shall allow only authorized switching mechanisms to switch between connected computers and shall explicitly prohibit or ignore unauthorized switching mechanisms. Authorized switching mechanisms shall require physical, zero-distance touch and include push-buttons, touch screen and mouse or cursor control. Unauthorized switching mechanisms include keyboard shortcuts, also known as “hotkeys,” automatic scanning and voice activation.	**O.AUTHORIZED_SWITCHING** mitigates this threat by preventing unauthorized switching methods that may cause user confusion and loss of situational awareness. A TOE with unauthorized switching mechanisms may cause misalignment between the actual TOE state and the user understanding of the TOE state.

Threat	Objective	Rationale
	O.NO_AMBIGUOUS_CONTROL If the TOE allows more than one authorized switching mechanism, only one method shall be operative at any given time to prevent ambiguous commands.	**O.NO_AMBIGUOUS_CONTROL** mitigates this threat by preventing TOE control mechanisms that are not well-defined. Ambiguous TOE control may cause cases of unintended switching of the TOE. The TOE controls must be unambiguous to prevent user confusion or misinterpretation of the TOE state.
	O.CONTINUOUS_INDICATION The TOE shall provide continuous visual indication of the computer to which the user is currently connected.	**O.CONTINUOUS_INDICATION** counters this threat by preventing the loss of TOE indications that may lead to user confusion. TOE monitoring must be shown at all times to reduce the risk of user confusion or misinterpretation of the TOE state. It should be noted that the user may take a break or get interrupted by multiple activities and therefore reliance on user memory to define the TOE state should be avoided.
	O.KEYBOARD_AND_MOUSE_TIED The TOE shall ensure that the keyboard and mouse devices are always switched together (i.e., they cannot be assigned to different peripheral groups) in order to prevent operational difficulties.	**O.KEYBOARD_AND_MOUSE_TIED** counters this threat by preventing a split between keyboard and mouse in the TOE, thus eliminating the potential user confusion caused by such a split. The TOE may enable grouping of peripheral devices (e.g., audio output may be switched separately from the keyboard). However, separation of the keyboard and the mouse may cause user confusion and could result in cases of unintended TOE switching.
	O.USER_AUTHENTICATION_TERMINATION If the TOE is emulating the user	**O.USER_AUTHENTICATION_TERMINATION** counters this threat by preventing an emulated user authentication device from having

Threat	Objective	Rationale
	authentication (multiple instances of the user authentication device are coupled to multiple computers at the same time) then once the authentication session is terminated (for example smart card removed), the session must terminate immediately in all connected computers.	an active authentication session in computers that are currently not selected by the TOE user. The TOE prevents this threat by terminating all actively connected authentication sessions simultaneously.
Peripheral Device Threats	Connected Peripheral Devices	
T.UNAUTHORIZED_DEVICES The use of unauthorized peripheral devices with a specific TOE peripheral port may allow unauthorized information flows between connected devices or enable an attack on the TOE or its connected computers.	O.PERIPHERAL_PORTS_ISOLATION The TOE shall prevent data flow between peripheral devices of different SPFs. TOE peripheral device ports of different SPFs shall be isolated (See Annex D, Table 1, Flows F and G).	**O.PERIPHERAL_PORTS_ISOLATION** mitigates this threat by eliminating potential electronic or logic linkage between the various TOE peripheral device ports. A TOE with peripheral port isolation will provide a higher level of protection from malicious or unauthorized peripheral devices.
	O.DISABLE_UNAUTHORIZED_PERIPHERAL The TOE shall only allow authorized peripheral device types (See Annex C) per peripheral device port; all other devices shall be identified and then rejected or ignored by the TOE.	**O.DISABLE_UNAUTHORIZED_PERIPHERAL** mitigates this threat by disabling unauthorized peripheral devices based on device profiling. Such peripheral device disabling is an effective means to prevent the use of unauthorized peripheral devices.
	O.DISABLE_UNAUTHORIZED_ENDPOINTS The keyboard and pointing device peripheral ports of the TOE shall reject any composite USB devices with endpoints other than those authorized for that specific port (See Annex C). Device rejection shall be accomplished either by completely disabling the connected device or disabling just the unauthorized endpoint(s). Similarly,	**O.DISABLE_UNAUTHORIZED_ENDPOINTS** assures that TOE connected peripheral devices with unauthorized functions (i.e., endpoints) are disabled and therefore would not be used. TOE rejection of unauthorized peripheral devices or functions within the devices is an effective means to prevent the intended or unintended use of such devices or

Threat	Objective	Rationale
	the TOE shall reject unauthorized peripheral devices connected via a USB hub (alternatively, the TOE may reject all USB hubs).	functions.
	O.USER_AUTHENTICATION_ADMIN If the TOE is capable of being configured after deployment with user authentication device qualification parameters then such configuration may only performed by an administrator.	**O.USER_AUTHENTICATION_ADMIN** mitigates this threat by assuring that only the administrator will be able to modify the accepted user authentication device profile (for a TOE that supports configurable user authentication device profiling). This prevents unauthorized users from modifying the profile and potentially allowing the use of a malicious or unsecure USB device.
T.AUTHORIZED_BUT_UNTRUSTED_DEVICES The use of authorized peripheral devices with the TOE may still cause unauthorized information flows between connected devices or enable an attack on the TOE or its connected computers. Such threats are possible due to known or unknown vulnerabilities or due to additional functions within the authorized peripheral device. All authorized peripheral devices are treated as untrusted under this PP.	O.KEYBOARD_MOUSE_EMULATED The TOE keyboard and pointing device functions shall be emulated (i.e., no electrical connection other than the common ground is allowed between peripheral devices and connected computers).	**O.KEYBOARD_MOUSE_EMULATED** assures that authorized devices such as keyboards and mice would not be misused to store data while switched between computers. Malicious computers connected to the TOE may exploit certain volatile or non-volatile memory effects in the connected keyboard and pointing device peripherals to temporarily store data. Such temporary data storage may be used to transfer data across connected computers. The use of emulated functions in the TOE is an effective method to assure that only the essential functions of the peripheral device will be supported.
	O.KEYBOARD_MOUSE_UNIDIRECTIONAL The TOE keyboard and pointing device data shall be forced to unidirectional flow from the peripheral device to the switched computer only. Such unidirectional	**O.KEYBOARD_MOUSE_UNIDIRECTIONAL** counters this threat by assuring that any attempt to store data in the keyboard and mouse by a compromised computer or TOE function will be blocked effectively through a physical barrier (as

Threat	Objective	Rationale
	flow enforcement shall be implemented in the TOE through physical (i.e., hardware) methods and not through logical (i.e., firmware dependent) methods (See Annex D, Table 1, Flow B).	opposed to software). The TOE shall force keyboard and mouse traffic to a unidirectional flow from the peripheral device to the connected computer only. If a reverse flow is authorized, then the keyboard and mouse may be misused by a compromised connected computer to store data and as a result, leak data between connected computers.
	O.UNIDIRECTIONAL_VIDEO TOEs that support VGA, DVI or HDMI video shall force native video peripheral data (i.e., red, green, blue, and TMDS lines) to unidirectional flow from the switched computer to the connected display device (See Annex D, Table 1, Flow I2).	**O.UNIDIRECTIONAL_VIDEO** mitigates the threat by preventing any potential reversal of the video path in the TOE that may be misused to transfer video or other data from computer-to-computer through the TOE. The TOE shall force native video traffic to unidirectional flow from the computer to the peripheral only. If reverse flow is authorized through the TOE, then logical tampering of the connected display may cause unauthorized data flow.
	O.UNIDIRERCTIONAL_EDID TOEs that support VGA, DVI, DisplayPort or HDMI video shall force the display EDID peripheral data channel to unidirectional flow and only copy once from the display to each one of the appropriate computer interfaces during the TOE power up or reboot sequence. The TOE must prevent any EDID channel write transactions initiated by connected computers.	**O.UNIDIRERCTIONAL_EDID** mitigates this threat by preventing misuse of shared displays to transfer data between connected computers. All display peripheral devices in use today support bidirectional interface protocols (e.g., EDID channel in DVI, VGA, HDMI interfaces or AUX channel in DisplayPort). If the TOE enforces a unidirectional data flow from a display to computers, then the display may not be misused to transfer data across connected computers.

Threat	Objective	Rationale
	O.DISPLAYPORT_AUX_FILTERING TOEs that support DisplayPort video shall prevent (i.e., filter or otherwise disable) the following auxiliary channel traffic: EDID write, USB, Ethernet, Audio return channel, UART and MCCS. Alternatively, the TOE may prevent the AUX channel from operating at Fast AUX speed (675/720 Mbps).	**O.DISPLAYPORT_AUX_FILTERING** counters this threat by avoiding the handling of AUX data other than the minimum required to support the video link. This AUX channel filtration assures that DisplayPort interfaces will not be misused by a compromised connected computer in an attempt to transfer data across connected computers.
	O.USER_AUTHENTICATION_RESET Unless the TOE emulating the user authentication function, upon switching computers, the TOE shall reset (turn off and then turn on) the power supplied to the user authentication device for at least 1 second.	**O.USER_AUTHENTICATION_RESET** mitigates the threat by preventing a potential data transfer between computers through known or unknown volatile memory in an authorized user authentication device.
Device Tampering	Tamper Mitigation	
T.LOGICAL_TAMPER An attached device (computer or peripheral) with malware or otherwise under the control of a malicious user could modify or overwrite code embedded in TOE volatile or non-volatile memory to allow unauthorized information flows between connected devices.	O.NO_TOE_ACCESS The TOE shall be designed so that access to the TOE firmware, software, or its memory via its accessible ports is prevented. This should be accomplished by offering no access to modify the TOE or its memory. To mitigate the risk that a potential attacker will tamper a TOE and then reprogram it with same or tampered functionality, the TOE external and internal interfaces shall be locked for code read and write. The programmable TOE components programming ports must be permanently disabled for both read and write operations. TOE operation code may not be upgradeable through any of the TOE external or internal ports.	**O.NO_TOE_ACCESS** counters the threat of logical tampering by assuring that the TOE does not support external or internal ports that provide programming access or firmware reading of internal components. Logical TOE tampering may be leveraged by the following TOE functions: 1. Internal or external access to the TOE firmware, software or memory. Such access may be used by potential attackers to modify the TOE security functions. 2. Programmer ports read or write access to the TOE circuitry. Such open access may be misused by

Threat	Objective	Rationale
		an attacker to read, modify and write TOE firmware in an attempt to clone, switch or tamper with a TOE. 3. Firmware upgrade function. Such functions may be misused by an attacker to read, modify and write TOE firmware in an attempt to clone, switch or tamper with a TOE.
T.PHYSICAL_TAMPER A malicious human agent could physically tamper with or modify the TOE to allow unauthorized information flows between connected devices.	O.ANTI_TAMPERING The TOE shall be physically enclosed so that any attempts to open or otherwise access the internals or modify the connections of the TOE would be evident. This shall be accomplished through the use of an always-on active anti-tampering system that serves to permanently disable the TOE should its enclosure be opened. The TOE shall use an always-on active anti-tampering system to permanently disable the TOE in case physical tampering is detected.	**O.ANTI_TAMPERING** mitigates this threat by assuring that any attempt to physically tamper with the TOE will cause it to become permanently disabled and will provide indications that the user cannot ignore.
	O.ANTI_TAMPERING_BACKUP_POWER The TOE anti-tampering system must have a backup power source to enable tamper detection while the TOE is unpowered.	**O.ANTI_TAMPERING_BACKUP_POWER** assures that the active anti-tampering function would continue to operate at all times – even when the TOE is powered off. TOE physical tampering protection must operate continuously to effectively prevent physical tampering while the TOE is powered off. Without this functionality, TOE power may be interrupted by the attacker in order to gain access to the TOE internal circuitry without triggering the anti-tampering

Threat	Objective	Rationale
		system.
	O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER A failure or depletion of the anti-tampering system backup power source shall trigger TOE to enter tampered state.	**O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER** counters this threat by ensuring that any case of backup power source failure causes the TOE to be permanently disabled to prevent an attacker from mounting an attack based on variables such as temperature exposure or time that may affect battery or super-capacitors used by the TOE anti-tampering system in order to gain access to the TOE internal circuitry. .
	O.ANTI_TAMPERING_INDICATION The TOE shall have clear user indications when tampering is detected.	**O.ANTI_TAMPERING_INDICATION** mitigates this threat by assuring that an event of physical TOE tampering while in service will be discovered by the user and reported to the proper security authorities within the organization. Clear TOE tampering indications, together with proper user training and internal procedures, will increase the probability that a TOE that has been tampered with will be properly detected.
	O.ANTI_TAMPERING_PERMANENTLY_ DISABLE_TOE Once the TOE anti-tampering is triggered, the TOE shall become permanently disabled. No peripheral-to-computers data flows shall be allowed.	**O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE** counters this threat by assuring that a TOE that has been tampered with will not continue to be used and possibly leak data. Permanent TOE disabling is critical in order to assure that the TOE would not be returned to normal service after it has been tampered with.
	O.TAMPER_EVIDENT_LABEL The TOE shall be identifiable as	**O.TAMPER_EVIDENT_LABEL** provides a higher level of assurance that the TOE was not physically

Threat	Objective	Rationale
	authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. The TOE manufacturer must maintain complete list of manufactured TOE articles and their respective identification markings' unique identifiers.	tampered with during transit or while in service. A tamper evident label is an effective means to provide clear visual indication of physical TOE tampering and also to assure the authenticity of the TOE.
T.REPLACEMENT A malicious human agent could replace the TOE during shipping, storage, or use with an alternate device that does not enforce the TOE security policies.	O.TAMPER_EVIDENT_LABEL The TOE shall be identifiable as authentic by the user and the user must be made aware of any procedures or other such information to accomplish authentication. This feature must be available upon receipt of the TOE and continue to be available during the TOE deployment. The TOE shall be labeled with at least one visible unique identifying tamper-evident marking that can be used to authenticate the device. Compliant TOE manufacturer must maintain complete list of manufactured TOE articles and their respective identification markings' unique identifiers.	**O.TAMPER_EVIDENT_LABEL** provides a higher level of assurance that the TOE was not physically tampered with during transit or while in service. A tamper evident label is an effective means to provide clear visual indication of physical TOE tampering and also to assure the authenticity of the TOE.
Unsafe Failure	Fail-Secure and Self-Testing	

Threat	Objective	Rationale
T.FAILED Detectable failure of a TOE causing an unauthorized information flow or weakening of TOE security functions.	O.SELF_TEST The TOE shall perform self-tests following power up or powered reset. The self-testing should at least cover: 1. The basic integrity of the TOE hardware and firmware; 2. The basic computer-to-computer isolation (See Annex D, Table 1, Flows J and K); and 3. The other critical security functions (i.e., user control and anti-tampering). For example, the following steps may be used to test basic isolation during power up: 1. The TOE is switched to channel 1; 2. A test packet is sent to the computer connected to channel 1; and The self-test function checks that all other ports are not receiving any data.	**O.SELF_TEST** mitigates the threat by increasing the probability that a critical TOE failure affecting security would be discovered. It also reduces the time that the TOE would continue to operate with such a failure. The TOE shall be equipped with a self-test function in order to detect failures of the underlying security mechanisms used by the TOE and in order to provide clear user indications in case such a failure is detected.
	O.SELF_TEST_FAIL_TOE_DISABLE Upon critical failure detection the TOE shall disable normal operation of the whole TOE or the respective failed component.	**O.SELF_TEST_FAIL_TOE_DISABLE** counters this threat by assuring that upon TOE failure detection, the user would not be able to continue using the TOE, thus reducing the potential security damage of a failure. If the TOE resumed normal operation after critical failure detection, the user may not be aware of the failure and as a result, data may leak through the TOE.
	O.SELF_TEST_FAIL_INDICATION The TOE shall provide clear and	**O.SELF_TEST_FAIL_INDICATION** counters this threat by providing

Threat	Objective	Rationale
	visible user indications in the case of a self-test failure. Such indication will preferably include details about the detected failure and its severity.	proper user guidance in case the TOE detects a failure. The indication should be used to guide immediate TOE disconnection from its working environment to prevent further potential security damages. If the TOE does not provide a clear failure indication after critical failure detection, the user may not be aware of the failure and as a result, data may leak through the TOE.

Table 18**:** Security Threats to Objectives Mapping

E.7 - Assumptions to Security Objectives for the Operational Environment

The following table contains a mapping of Assumption to Objectives for the Operational Environment.

Assumption	Objective	Rationale
A.NO_TEMPEST It is assumed that the computers and peripheral devices connected to the TOE are not TEMPEST approved.	OE. NO_TEMPEST The operational environment will not require the use of TEMPEST approved equipment.	**OE. NO_TEMPEST** upholds this assumption by ensuring that the operational environment does not impose requirements for TEMPEST approved equipment.
A.NO_SPECIAL_ANALOG_CAPABILITIES It is assumed that the computers connected to the TOE are not equipped with special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.	OE. NO_SPECIAL_ANALOG_ CAPABILITIES The operational environment will not require special analog data collection cards or peripherals such as: Analog to digital interface, high performance audio interface, Digital Signal Processing function, and analog video capture function.	**OE. NO_SPECIAL_ANALOG_CAPABILITIES** upholds this assumption by ensuring that the operational environment does not impose requirements for special analog data collection cards or peripherals.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	OE.PHYSICAL The operational environment will provide physical security, commensurate with the value of the TOE and the data it contains.	**OE.PHYSICAL** upholds this assumption by ensuring that the operational environment provides physical security, commensurate with the value of the TOE and the data it contains.
A.TRUSTED_ADMIN TOE Administrators and users are trusted to follow and apply all guidance in a trusted manner.	OE.TRUSTED_ADMIN The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.	**OE.TRUSTED_ADMIN** upholds this assumption by ensuring that only appropriately trained and trusted administrators and users will be exercising TOE functions.
A.TRUSTED_CONFIG	OE.TRUSTED_ADMIN	**OE.TRUSTED_ADMIN** upholds

Assumption	Objective	Rationale
Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.	The operational environment will ensure that appropriately trained and trusted TOE Administrators and users are available to administer, configure and use the TOE.	this assumption by ensuring that only appropriately trained and trusted administrators and users will be configuring the TOE.

Table 19**:** Assumptions to Security Objectives for the Operational Environment

E.8 Security Objectives to Security Requirements

The following table contains a mapping of Security Objectives for the TOE to Security Functional Requirements.

Objective	SFRs	Notes

[O.COMPUTER_INTERFACE_ISOLATION]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.COMPUTER_INTERFACE_ISOLATION_TOE_UNPOWERED]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.USER_DATA_ISOLATION]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.NO_USER_DATA_RETENTION]	FDP_RIP.1	
[O.PURGE_TOE KB_DATA_WHILE_SWITCHING]	FDP_RIP.1	

[O.NO_DOCKING_PROTOCOLS]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.NO_OTHER_EXTERNAL_INTERFACES]	FDP_IFC.1(2) FDP_IFF.1. (2)	

[O.NO_ANALOG_AUDIO_INPUT]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.UNIDIRECTIONAL_AUDIO_OUT]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.COMPUTER_TO_AUDIO_ISOLATION]	FDP_IFC.1(1)
	FDP_IFF.1(1)
		This objective is touched on, but not met by these SFRs.

[O.USER_AUTHENTICATION_ISOLATION]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.USER_AUTHENTICATION_RESET]	FDP_IFF.1. (1) FTA_ATH_EXT.1	

[O.USER_AUTHENTICATION_TERMINATION]	FDP_IFF.1.3(1) FTA_ATH_EXT.2	
[O.USER_AUTHENTICATION_ADMIN]	FMT_SMF.1 b FMT_MOF.1 FMT_SMR.1	

[O.AUTHORIZED_SWITCHING]	FDP_IFC.1(2)
	FDP_IFF.1(2)	

[O.NO_AMBIGUOUS_CONTROL]	FDP_IFC.1(2)
	FDP_IFF.1(2)	

[O.CONTINUOUS_INDICATION]	FTA_CIN_EXT.1	
[O.KEYBOARD_AND_MOUSE_TIED]	FDP_ACC.1 FDP_ACF.1	

[O.NO_CONNECTED_COMPUTER_CONTROL]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.PERIPHERAL_PORTS_ISOLATION]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.DISABLE_UNAUTHORIZED_PERIPHERAL]	FDP_ACC.1 FDP_ACF.1	
[O.DISABLE_UNAUTHORIZED_ENDPOINTS]	FDP_ACC.1 FDP_ACF.1	
[O.KEYBOARD_MOUSE_EMULATED]	FDP_ACC.1 FDP_ACF.1	
[O.KEYBOARD_MOUSE_UNIDIRECTIONAL]	FDP_ACC.1 FDP_ACF.1	

[O.UNIDIRECTIONAL_VIDEO]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.UNIDIRERCTIONAL_EDID]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.DISPLAYPORT_AUX_FILTERING]	FDP_IFC.1(1)
	FDP_IFF.1(1)	

[O.NO_TOE_ACCESS]	FPT_PHP.3 FPT_FLS.1	
[O.TAMPER_EVIDENT_LABEL]	FPT_PHP.1	
[O.ANTI_TAMPERING]	FPT_PHP.3	
[O.ANTI_TAMPERING_BACKUP_POWER]	FPT_PHP.3	Implied, but not directly stated in the SFR
[O.ANTI_TAMPERING_BACKUP_FAIL_TRIGGER]	FPT_PHP.3	
[O.ANTI_TAMPERING_INDICATION]	FPT_PHP.1	
[O.ANTI_TAMPERING_PERMANENTLY_DISABLE_TOE]	FPT_PHP.3 FPT_FLS.1	
[O.SELF_TEST]	FPT_TST.1	
[O.SELF_TEST_FAIL_TOE_DISABLE]	FPT_TST.1 FPT_FLS.1	
[O.SELF_TEST_FAIL_INDICATION]	FPT_TST.1	

Table 20: Security Objectives to Requirements

E.9 Security Requirements to Tests

The following table contains a mapping of Security Requirements for the TOE to specific tests / deliverables.

Test SFR	4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9	4.10	4.11	4.12	4.13	4.14	4.15	4.16	Letter of volatility	Isolation Analysis
FDP_IFC.1 (1)	●	●	●	●	●	●	●	●										
FDP_IFF.1 (1)	●	●	●	●	●	●	●	●										
FDP_IFC.1 (2)		●	●	●	●	●		●	●	●	●							●
FDP_IFF.1 (2)		●	●	●	●	●		●	●	●	●							
FDP_ACC.1		●	●															
FDP_ACF.1		●	●															
FDP_RIP.1												●					●	
FPT_PHP.1													●					
FPT_PHP.3													●					
FPT_FLS.1														●				
FPT_TST.1														●				
FTA_CIN_EXT.1															●			
FAU_GEN.1																●		
FIA_UID.2				●	●													
FIA_UAU.2					●													
FMT_MOF.1				●	●													
FMT_SMF.1		●	●	●	●													
FMT_SMR.1																		
FTA_ATH_EXT.1					●													
FTA_ATH_EXT.2					●													

Table 21: Security Requirements to Tests and Deliverables

ANNEX F: OPTIONAL REQUIREMENTS

As indicated in the introduction to this PP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this PP. Additional requirements are specified in Annexes F and G.

The requirements in this Annex may be included in the ST, but are not required in order for a TOE to claim conformance to this PP.

F.1 - Optional TOE Configuration

F.1.1 Overview

In the development of this PP there was an attempt to provide the users with better functionality and longer product life-span. This PP covers a wider range of PSS products and larger set of PSS functions. Still, in order to preserve the security functions mandatory by this PP, TOE firmware updates are not allowed.

However, TOE configuration may be required and therefore is allowed under certain conditions. PSS configuration may be required to allow longer product life-span through higher deployment flexibility and to provide wider product support for new peripheral devices. TOE configuration options may not be used to load new firmware into the TOE. The TOE must use existing firmware already installed during TOE production, but certain TOE operational parameters may be modified to meet these goals.

The support of user authentication devices in a PSS is specifically challenging. From a security standpoint it is desirable for the TOE to analyze and qualify each connected USB device prior to allowing it to connect to any computer to prevent connection or sharing of a malicious or unauthorized device. In the case of a USB keyboard and mouse, this device function qualification or filtering is relatively straight-forward. In the case of a USB user authentication device however, the qualification process may be much more complex as devices tend to be increasingly varied. The lack of proper standardization of the user authentication devices sold today causes significant technical challenges to positively identify these complex devices using a fixed set of rules. In order to provide future-proof user authentication device filtration functionality, administrator configurable device profiling must be supported.

Therefore, as an option, the TOE may support a configurable user authentication device profiling or filtering function (CDF). This function may be provided to allow administrators to configure the TOE to accept or reject specific USB devices. This CDF function may be necessary in order to secure the TOE and its connected computers while allowing complex user authentication devices to be qualified and used.

Several types of TOE configuration are allowed, but not required, under this PP:

1. User configuration to perform customizations and adaptations of the TOE to the specific user environment. TOE user configuration may not alter security related functions.

2. Administrator configuration of the user authentication device filtration parameters. This process may affect TOE security and therefore only authorized administrators may perform these activities.
3. Administrator configuration to perform other types of customizations and adaptations of the TOE to the specific user environment. These processes may have minimal effect on TOE security and therefore only authorized administrators may perform these activities.

TOE configuration methods may vary according to the specific implementation, and may range from simple keyboard shortcuts, to use of a connected computer application. Configuration may be temporary by nature (for example, a user configuring the mouse cursor speed) or permanent. Permanent configurations may be stored in the TOE non-volatile memory in order to maintain TOE configuration and state following power cycling.

If the TOE supports activities that require the actions of an authorized administrator, the following SFRs must be claimed:

- FAU_GEN.1 – The actions of the authorized administrator must be auditable. No specific SFRs are required to detail the methods for storing and reading audit entries; however, this information must be included in the TSS
- FIA_UID.2 and FIA_UAU.2 – Authorized administrators must be appropriately identified and authenticated to perform any action identified as an administrative activity
- FMT_MOF.1, FMT_SMF.1 and FMT_SMR.1 – The administrative functions are described in FMT_MOF.1 and FMT_SMF.1. The administrative role or roles are described in FMT_SMR.1.

F.1.2 Class: Security Audit (FAU)

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*administrator login, administrator logout, and* [assignment: all administrative functions claimed in FMT_MOF.1 and FMT_SMF.1]]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other information].

Assurance Activity

TSS

The evaluator shall verify that the TSS describes the audit functionality including which events are audited, what information is saved in each record type, how the records are stored, the conditions in which audit records are overwritten, and the means by which the audit records may be read. Although the TOE may provide an interface for an administrator to view the audit records, this is not a requirement.

Test

The evaluator shall perform each of the auditable functions to succeed, and where possible, to fail. The evaluator shall use the means described in the TSS to access the audit records and verify that each of the events has been recorded, with all of the expected information.

F.1.3 Class: Identification and authentication (FIA)

FIA_UAU.2 User identification before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application notes:

The Administrator shall be authenticated through logon or a specially assigned key before access to administrative functions is provided by the TOE.

Assurance Activity

Refer to the assurance activities of FMT_MOF.1.1 above.

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application notes:

The Administrator shall be identified through logon or a specially assigned key before access to administrative functions is provided by the TOE.

Assurance Activity

Refer to the assurance activities of FMT_MOF.1.1 above.

F.2 – Optional Management

F.2.1 Class: Security Management (FMT)

The TOE is not required to maintain a separate management role. However, it may provide the following optional management roles:

a. **Administrative configuration** - Functionality to configure certain aspects of TOE operation that should not be available to the general user population. Requires administrator identification and authentication (logon).
b. **User configuration** - Functionality to enable user configuration of certain aspects of TOE operation. Shall be available to all users. No user identification or authentication is required by this PP.

Management of Functions in TSF (FMT_MOF)

FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles; and
FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to [*perform*] the functions [selection: *modify TOE user authentication device filtering (CDF) whitelist and blacklist*] to [*the authorized administrators*].

Assurance Activity

TSS

The evaluator shall verify that the TSS describes the mechanism for preventing non-administrators from accessing the administrative functions stated above.

Guidance

The evaluator shall check the user and administrative guidance to verify that the administrative functions defined above are only available to identified administrators.

Test

The testing for this SFR is covered in Tests 4.5 above and Test F1 below.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TOE shall be capable of performing the following management functions:

a. [Conditional] If the TOE supports configurable user authentication device filtering (CDF) – then it shall provide authorized administrators the option to assign whitelist and blacklist definitions for the TOE user authentication device qualification function,
b. [Assignment: any additional TOE management functions].

Application Notes:

If there are additional management functions performed by the TOE (including those specified in Section 4.2.4, FMT_SMF), they should be added in the assignment.

Assurance Activity

TSS

The evaluator shall check to ensure the TSS describes the various administrator and user TOE configurations and how they are used by the TOE.

Guidance

The evaluator shall check to make sure that every management function mandated in the ST for this requirement are described in the operational guidance and that the description contains the information required to perform the management duties associated with each management function.

Test

The testing for this SFR is covered in:

- FMT_SMF.1.1 a - Test F1 below.
- FMT_SMF.1.1 b - Test 4.5 Part 5 above.

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*users, administrators*].

Application notes:

There is no requirement in this PP that user shall be authenticated by the TOE.

Assurance Activity

Refer to the assurance activities of FMT_MOF.1.1 above.

ANNEX G: SELECTION-BASED REQUIREMENTS

As indicated in the introduction to this PP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this PP. There are additional requirements based on selections in the body of the PP: if certain selections are made, then additional requirements below will need to be included.

G.1 - Class FTA_ATH_EXT: User Authentication Device Reset and Termination

G.1.1 User authentication device reset

[Conditional] This SFR is applicable only for a TOE that supports a user authentication device that is not emulated and not built-in to the TOE.

FTA_ATH_EXT.1 User authentication device reset

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.1.1 The TSF shall reset the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another.

Application Notes:

It is assumed that the user authentication device is not powered by an external power source.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes how the TOE resets the power to the user authentication device. The TSS shall also describe the amount of capacitance in the TOE and how it will affect the voltage decrease on an average user authentication device. Capacitance shall be small enough to assure that low-power devices would reach less than 2.0 V during that one second power reset.

Guidance

The evaluator shall verify that the user guidance provides information about the prohibited use of user authentication devices with external power sources.

Test

Testing for this SFR is covered by Test 4.5 Part 1 above.

G.1.2 User Authentication Device Session Termination

[Conditional] This SFR is applicable only for a TOE that supports a user authentication device function that is emulated.

FTA_ATH_EXT.2 User authentication device session termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.2.1 The TSF shall ensure that the user authentication session is terminated in all connected computers when the user terminates one authentication session or when the TOE is powered off.

Application Notes:

The user authentication device is no longer considered to be in use when the session is manually terminated by the user. An example of this is the user removing a smartcard.

Assurance Activity

TSS

The evaluator shall verify that the TSS describes how the TOE terminates all authentication sessions when one session is terminated by the user. For example, when the TOE is switched to computer #1 and computers #2, #3 and #4 have active authentication sessions, the TSS would describe the chain of events that would result when the user removes the smart-card from the reader. Additionally, the TSS shall specify the mechanism that prevents active sessions from continuing while the TOE is powering down.

Guidance

The evaluator shall verify that the user guidance provides information describing user authentication session termination both by the user and by the TOE at power down.

Test

Testing for this SFR is covered by Test 4.5 Part 2 above.

ANNEX H: EXTENDED COMPONENTS DEFINITION

H.1 Family FTA_CIN_EXT: Continuous Indications

The extended family belongs to the FTA: TOE Access class and has been created to provide for a continuous indication of the connected computer port group. FTA_CIN_EXT.1 is modeled after FTA_TAB.1.

Family Behavior

This family defines the requirements for continuous indications. This family may be used to specify that the TOE must provide an indication of its operational state.

Component Leveling

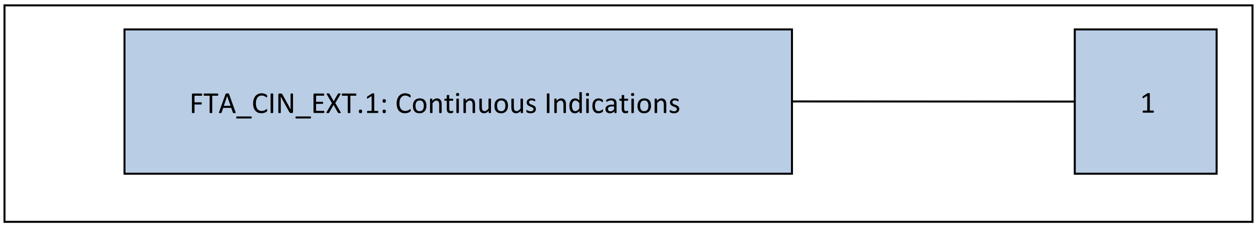


Figure 9: FTA_CIN_EXT.1: Continuous Indications

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_CIN_EXT.1.1 The TSF shall display a continuous visual indication of the computer to which the user is currently connected, including on power up, [selection: *on reset*].

H.4 Class FTA_ATH_EXT: User Authentication Device Reset and Termination

The extended family belongs to the FTA: TOE access class and has been created to describe reset and termination activities associated with the use of a user authentication device peripheral. Both FTA_ATH_EXT.1 and FTA_ATH_EXT.2 are modeled after FTA_SSL.4, User-initiated termination.

Family Behavior

This family defines the requirements for the use of an authentication device, including the reset and termination of authentication devices.

Component Leveling

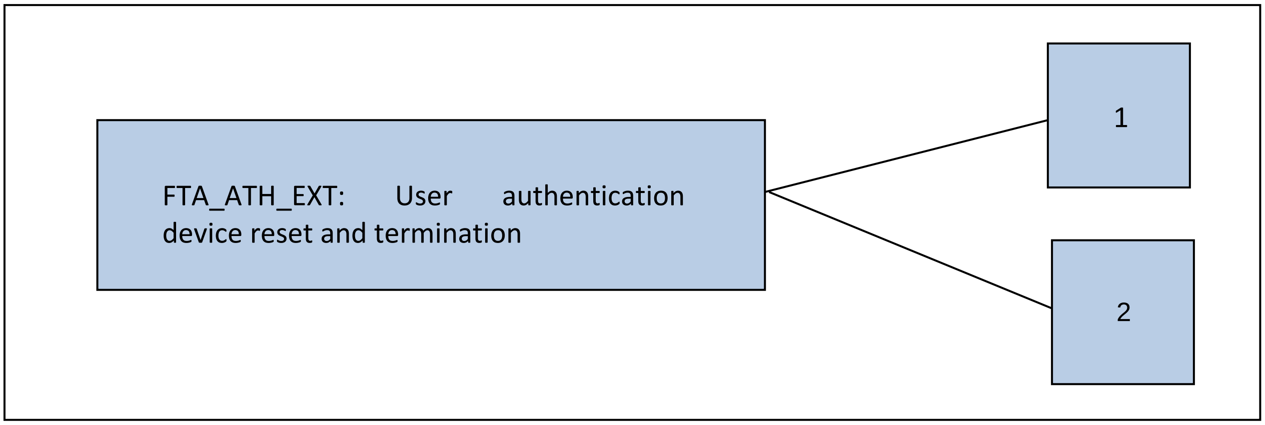

FTA_ATH_EXT: User authentication device reset and termination
1
2

Figure 10: FTA_ATH_EXT.1: User authentication device reset and termination

Management

There are no management activities foreseen for either FTA_ATH_EXT.1 or FTA_ATH_EXT.2.

Audit

There are no auditable events foreseen for either FTA_ATH_EXT.1 or FTA_ATH_EXT.2.

FTA_ATH_EXT.1 User authentication device reset

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.1.1 The TSF shall reset the power supplied to the user authentication device for at least one second when the user switches the device from one computer to another.

Application Notes:

It is assumed that the user authentication device is not powered by an external power source.

User Authentication Device Session Termination

FTA_ATH_EXT.2 User authentication device session termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_ATH_EXT.2.1 The TSF shall ensure that the user authentication session is terminated in all connected computers when the user terminates one authentication session or when the TOE is powered off.

Application Notes:

The user authentication device is no longer considered to be in use when the session is manually terminated by the user. An example of this is the user removing a smartcard.

ANNEX I: ASSURANCE ACTIVITIES TEST ENVIRONMENT

I.1 General

This appendix provides a list of equipment and software that is required for testing. The information provided here includes examples of software and hardware products that may be used; however, the evaluator may select other products as long they are suited for the required testing.

I.2 Disclaimer

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by NIAP of any non-Federal entity, event, product, service, or enterprise.

I.3 Standard Equipment

The following table lists the equipment required for a standard test. This, or equivalent defined set of equipment and software may be used.

No.	Equipment	Comments
1.	TOE	Several samples will be required. Testing of anti-tampering features will destroy several devices.
2.	TOE power supply or power cables	
3.	Compatible computer displays	At least 3-4. Avoid using adaptors for testing.
4.	USB keyboard	
5.	PS/2 keyboard	If applicable
6.	USB mouse (preferably an optical mouse with colored visible light)	
7.	PS/2 mouse	If applicable

8.	User authentication device	If applicable
9.	TOE computer interface cables	The cables should be supplied with the TOE, or recommended for use with the TOE.
10.	Computers	Computers shall have at least the following software: a. Operating system (Windows, Linux etc.); b. Real-time device information console; c. Text editor; d. Sound recording application; e. Media player with video to play; and f. User authentication device driver and application (e.g., Windows logon using smartcard).

Table 22: Standard equipment required for Assurance Activities Testing

I.4 Special Equipment per Test

The following table specifies the special equipment / software needed for each test.

Test	USB protocol analyzer device (sniffer)	USB protocol analyzer software	USB storage device	USB Audio device	USB Hub	USB Overload plug	Power supply with current limit	USB Type B plug	Amplified speakers	Tone generator software application	Keyboard emulator software application	USB Generator	Computer microphone (analog)	Open 3.5 mm stereo plug	Digital Voltmeter	Dynamic headphones	DisplayPort AUX channel analyzer	Display having DP 1.2 interface	MCCS control console software application	DisplayPort source device	EDID reading and parsing software	Audio signal generator	USB Printer	USB Camera	USB Composite device evaluation board	Oscilloscope	Armed TOE sample with open enclosure
4.1																											
4.2	●	●	●	●	●						●	●											●	●	●		
4.3	●	●	●	●	●						●	●											●	●	●		

4.4																●	●	●	●	●					●	
4.5	●	●	●	●	●									●							●	●	●	●		
4.6								●	●			●	●	●	●						●				●	
4.7																											
4.8	●	●				●	●	●																			
4.9																											
4.10									●																		
4.11	●	●																									
4.12																											
4.13																											
4.14																											●
4.15																											

Table 23: Special equipment required for Assurance Activities Testing

I.5 Additional Information Regarding Special Equipment

The following text and images provide some examples of equipment and software that may be used to perform the required testing. The inclusion of any specific product is not meant as an endorsement of the product, but as a sample device that may be used for testing.

I.5.1 Real-Time hardware information console

The Real-Time hardware information console may be Device Manager in the Windows OS. Alternatively, the evaluator may use similar Linux or other operating system tools such as: Gnome Device Manager, KDE's KInfoCentre, Ubuntu's Device Manager, SUSE's Yast and Mandriva's Control Centre.

I.5.2 USB Overload Plug

A USB Overload plug can be easily made at the lab using a power resistor (see: http://www.digikey.com/product-detail/en/TMC0102R500FE02/TMC10-2.5-ND/269926) and any standard USB cable (Type-A to Type-B). The Type-B side can be cut and the remaining wire with Type-A can be soldered to the resistor. The black wire should be soldered to one resistor side and red wire to the other. Alternatively, USB dummy load units like the one in the image below may be purchased on-line.

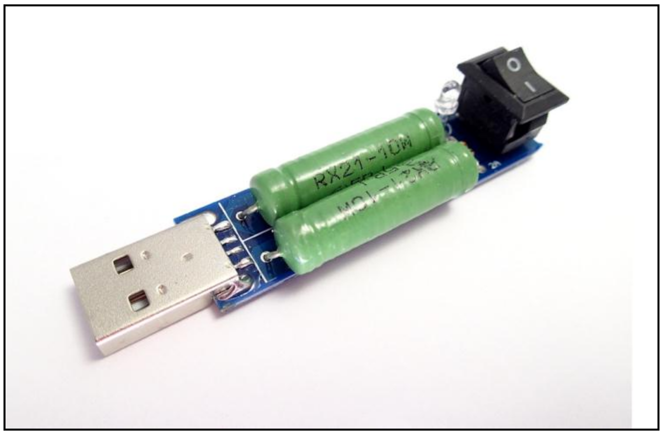


Figure 11: USB Overload plug

I.5.3 USB sniffer / protocol analyzer device

An example of a low-cost USB sniffer /protocol analyzer device is the International Test Instruments 1480A, see: http://www.internationaltestinstruments.com/products/97-1480a-usb-20-protocol-analyzer.aspx

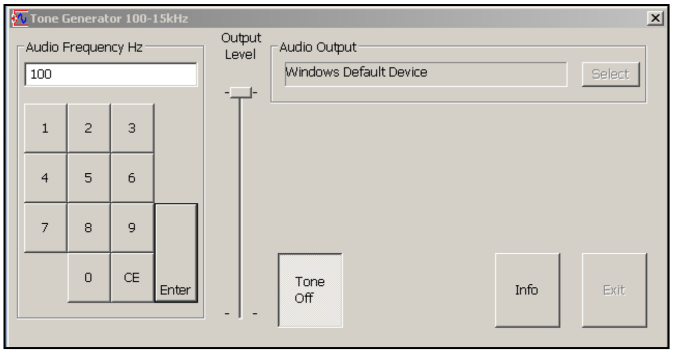
I.5.4 USB Protocol Analyzer Software

Free USB Protocol analyzer software can be downloaded from: http://freeusbanalyzer.com/

I.5.5 Tone Generator Software Application

Free Windows tone generator software can be downloaded from: http://www.ringbell.co.uk/software/audio.htm

The figure below shows a screen capture of a tone generator application set to generate a 100 hertz sine wave at maximum level:


Tone Generator 100-15kHz

Audio Frequency Hz: 100

Output Level

Audio Output: Windows Default Device

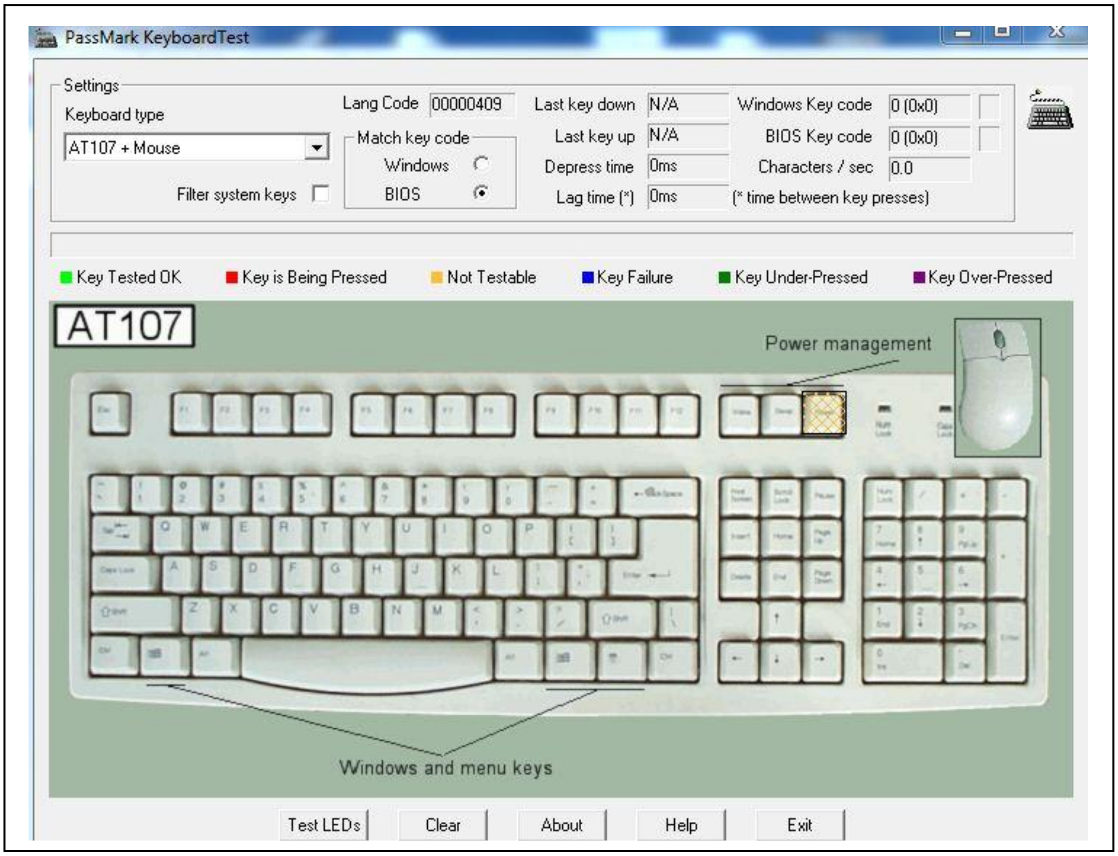
Figure 12: Tone generator screenshot

I.5.6 Amplified speakers

The tests in this PP depend upon the use of high-quality system 2.1 standard and higher amplified speakers with a separate subwoofer. Examples include Harman Kardon Soundsticks III 2.1 Channel Multimedia Speaker System with Subwoofer, Altec Lansing VS2621 2.1 Channel Speaker System, or Creative Inspire T6300 5.1 Multimedia Speaker System.

I.5.7 USB keyboard emulation software

PassMark KeyboardTest™ version 3.0 (http://www.passmark.com/products/keytest.htm) shows the graphical interface required to simulate Caps Lock and mouse keys activities.


PassMark KeyboardTest

Settings

Keyboard type: AT107 + Mouse

Filter system keys □

Lang Code: 00000409

Match key code: Windows ○ BIOS ●

Last key down: N/A

Last key up: N/A

Depress time: 0ms

Lag time (*): 0ms

Windows Key code: 0 (0x0)

BIOS Key code: 0 (0x0)

Characters / sec: 0.0

(* time between key presses)

🟩 Key Tested OK 🟥 Key is Being Pressed 🟨 Not Testable 🟦 Key Failure 🟩 Key Under-Pressed 🟪 Key Over-Pressed

Figure 13: PassMark KeyboardTest™ version 3.0 user interface screen capture

I.5.8 USB Type-B Plug

This is a common part that may be purchased on-line: http://www.digikey.com/product-detail/en/A-USBPB-R/AE10178-ND/1119639

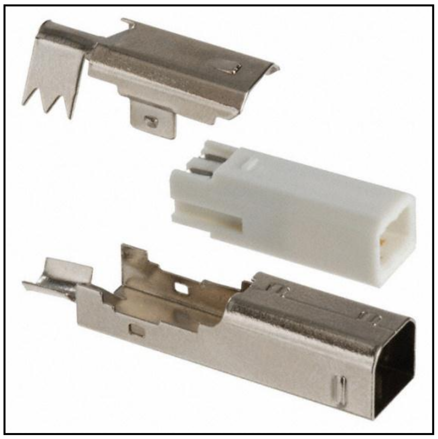
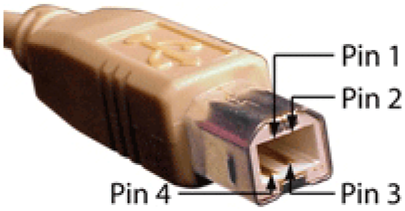


Figure 14: USB Type-B plug



5V power shall be connected to Vbus (pin 1) and the negative side of the power supply should be connected to pin 4.

I.5.9 Stereo audio plug 3.5 millimeter

These can be found in many on-line stores, including http://www.digikey.com/product-detail/en/SP-3501/CP-3502-ND/96987

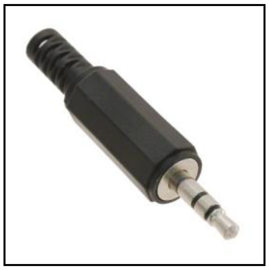
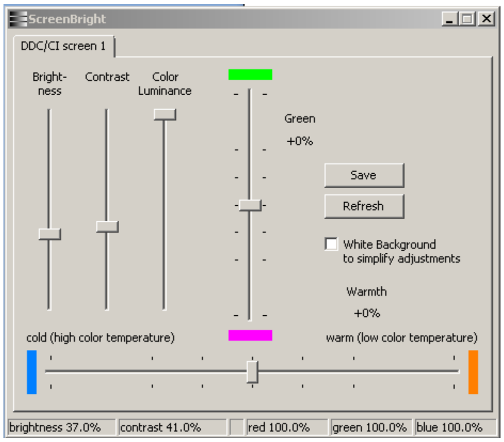


Figure 15: 3.5mm stereo plug

I.5.10 MCCS control Software Application

Free software to control display MCCS can be found here: http://download.cnet.com/Screen-Bright/3000-18514_4-76168604.html



ScreenBright
DDC/CI screen 1
Bright-ness
Contrast
Color Luminance
Green
Save
Refresh
White Background to simplify adjustments
Warmth
cold (high color temperature)
warm (low color temperature)

Green +0%

□ White Background to simplify adjustments

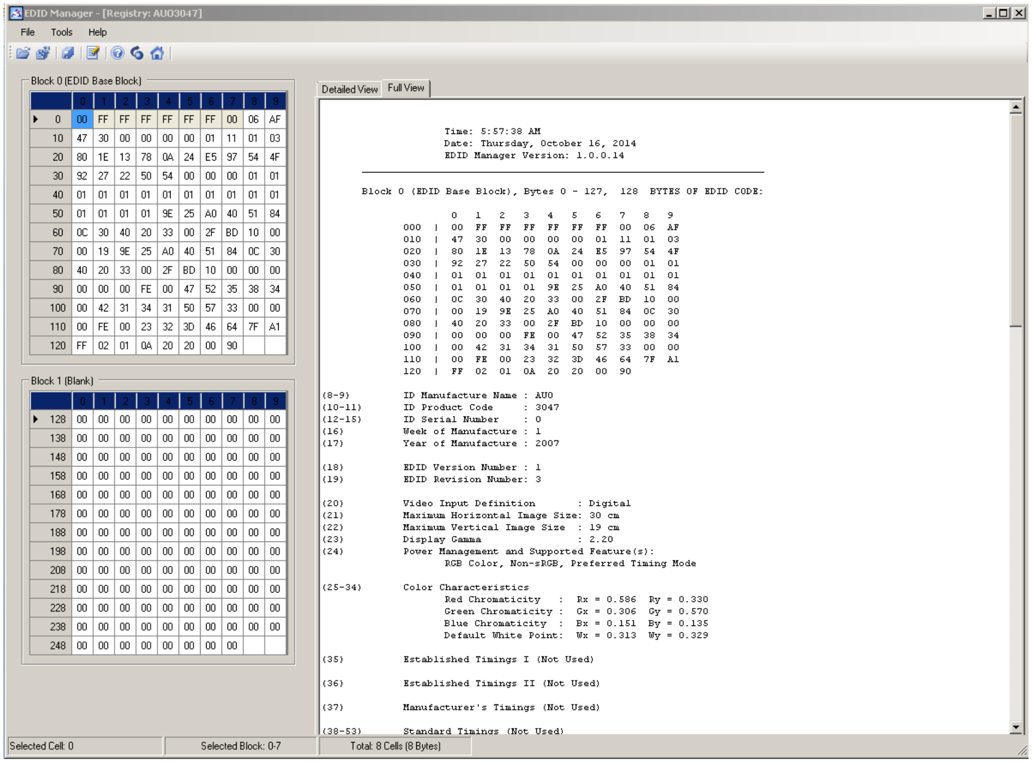
Warmth +0%

brightness 37.0% | contrast 41.0% | red 100.0% | green 100.0% | blue 100.0%

Figure 16: ScreenBright MCCS control console screen capture

I.5.11 Software to read and parse display EDID

Free Windows software to read and parse display EDID can be found here: http://www.extron.com/download/dltrack.aspx?file=EDID_ManagerV1x0.exe&id=38772



Block 0 (EDID Base Block)

	0	1	2	3	4	5	6	7	8	9
0	00	FF	FF	FF	FF	FF	FF	00	06	AF
10	47	30	00	00	00	00	01	11	01	03
20	80	1E	13	78	0A	24	E5	97	54	4F
30	92	27	22	50	54	00	00	00	01	01
40	01	01	01	01	01	01	01	01	01	01
50	01	01	01	01	9E	25	A0	40	51	84
60	0C	30	40	20	33	00	2F	BD	10	00
70	00	19	9E	25	A0	40	51	84	0C	30
80	40	20	33	00	2F	BD	10	00	00	00
90	00	00	00	FE	00	47	52	35	38	34
100	00	42	31	34	31	50	57	33	00	00
110	00	FE	00	23	32	3D	46	64	7F	A1
120	FF	02	01	0A	20	20	00	90		

Block 1 (Blank)

	0	1	2	3	4	5	6	7	8	9
128	00	00	00	00	00	00	00	00	00	00
138	00	00	00	00	00	00	00	00	00	00
148	00	00	00	00	00	00	00	00	00	00
158	00	00	00	00	00	00	00	00	00	00
168	00	00	00	00	00	00	00	00	00	00
178	00	00	00	00	00	00	00	00	00	00
188	00	00	00	00	00	00	00	00	00	00
198	00	00	00	00	00	00	00	00	00	00
208	00	00	00	00	00	00	00	00	00	00
218	00	00	00	00	00	00	00	00	00	00
228	00	00	00	00	00	00	00	00	00	00
238	00	00	00	00	00	00	00	00	00	00
248	00	00	00	00	00	00	00	00		

```
                 Time: 5:57:38 AM
                 Date: Thursday, October 16, 2014
                 EDID Manager Version: 1.0.0.14
      ______________________________________________________

      Block 0 (EDID Base Block), Bytes 0 - 127,  128  BYTES OF EDID CODE:

                     0   1   2   3   4   5   6   7   8   9
            000  |  00  FF  FF  FF  FF  FF  FF  00  06  AF
            010  |  47  30  00  00  00  00  01  11  01  03
            020  |  80  1E  13  78  0A  24  E5  97  54  4F
            030  |  92  27  22  50  54  00  00  00  01  01
            040  |  01  01  01  01  01  01  01  01  01  01
            050  |  01  01  01  01  9E  25  A0  40  51  84
            060  |  0C  30  40  20  33  00  2F  BD  10  00
            070  |  00  19  9E  25  A0  40  51  84  0C  30
            080  |  40  20  33  00  2F  BD  10  00  00  00
            090  |  00  00  00  FE  00  47  52  35  38  34
            100  |  00  42  31  34  31  50  57  33  00  00
            110  |  00  FE  00  23  32  3D  46  64  7F  A1
            120  |  FF  02  01  0A  20  20  00  90

(8-9)       ID Manufacture Name : AUO
(10-11)     ID Product Code     : 3047
(12-15)     ID Serial Number    : 0
(16)        Week of Manufacture : 1
(17)        Year of Manufacture : 2007

(18)        EDID Version Number : 1
(19)        EDID Revision Number: 3

(20)        Video Input Definition       : Digital
(21)        Maximum Horizontal Image Size: 30 cm
(22)        Maximum Vertical Image Size  : 19 cm
(23)        Display Gamma                : 2.20
(24)        Power Management and Supported Feature(s):
                   RGB Color, Non-sRGB, Preferred Timing Mode

(25-34)     Color Characteristics
                   Red Chromaticity   :  Rx = 0.586  Ry = 0.330
                   Green Chromaticity :  Gx = 0.306  Gy = 0.570
                   Blue Chromaticity  :  Bx = 0.151  By = 0.135
                   Default White Point:  Wx = 0.313  Wy = 0.329

(35)        Established Timings I (Not Used)

(36)        Established Timings II (Not Used)

(37)        Manufacturer's Timings (Not Used)

(38-53)     Standard Timings (Not Used)
```

Selected Cell: 0 | Selected Block: 0-7 | Total: 8 Cells (8 Bytes)

Figure 17: Extron EDID Manager application-screen-capture

I.5.12 DisplayPort AUX channel analyzer

An example of DisplayPort AUX channel analyzer is Unigraf DPA-400 (http://www.unigraf.fi/products/testing-display-electronics/displayport/dp-aux-channel-monitor).

Note that other analyzers with support for DisplayPort version 1.2 may be used.

I.5.13 USB Composite Device Evaluation Board

An example of a USB evaluation board that can be set up to provide a composite device is Atmel EVK1100. See link: http://www.digikey.com/product-search/en?mpart=ATEVK1100&vendor=313

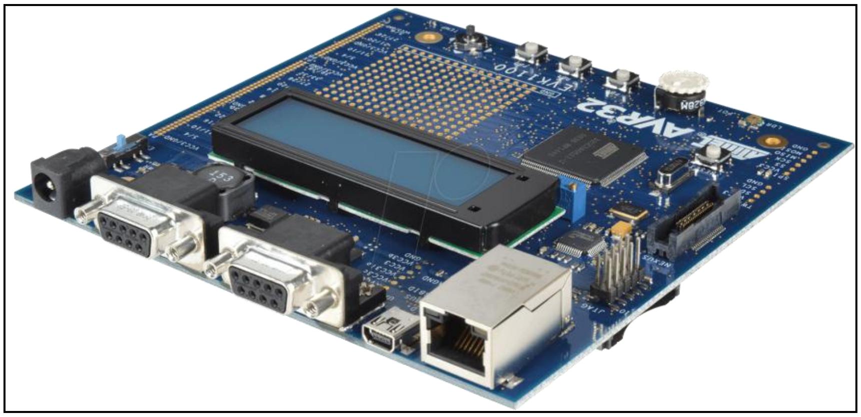


Figure 18: Atmel EVK1100 Evaluation Board

Note: Refer to document: http://www.atmel.com/Images/doc8445.pdf for detailed instructions on how to set the board up to operate as a composite device.

Other products and evaluation boards may be used if they are capable of generating a composite USB device with HID.

I.5.14 Oscilloscope

Any general purpose single channel or more oscilloscope may be used. The sampling frequency shall be 500MHZ, 500MS/S or higher. Both single ended and differential (for video testing) probes are required. An example of a compatible oscilloscope is the Tektronix TDS 510A. Note that a higher bandwidth oscilloscope may be required to properly detect DisplayPort signals (if applicable). An example of a compatible higher bandwidth oscilloscope is the Agilent DSO81004A Infinium Oscilloscope, 10 GHz, 4CH, 40GSa/s.

I.5.15 Audio Signal Generator

Any audio signal generator capable of generating a sine wave with positive negative bias from DC up to 100 KHz or more may be used. An example of a compatible signal generator is the HP-8904A Signal Generator Sine wave signals from DC to 100 KHz.

ANNEX J: ISOLATION DOCUMENTATION AND ASSESSMENT

J.1 General

The documentation of the isolation should be detailed enough that, after reading, the evaluator will thoroughly understand the isolation concepts and implementation in the TOE and why it can be relied upon to provide proper isolation between connected computers. This documentation should include multiple detailed sections: design description, isolation means justification, firmware dependencies, and single failure analysis.

This documentation is not required to be part of the TSS and may be kept confidential.

J.2 Design Description

The documentation shall include the design of all user data paths inside the TOE as a whole, including the interaction between the various data paths and their primary components (microcontrollers or programmable logic). It shall have one or more block diagrams showing the different data paths in the TOE and any parts that may translate, emulate, switch, forced into unidirectional flow or otherwise affect these data streams. It shall also describe the operation of one of the main components in the data paths to include how it works, how isolation is kept, and how power source or power loading may affect isolation between these data paths. The documentation should walk through the flow of each data stream (keyboard, mouse, display video, display EDID, audio etc.) and describe each component that may handle more than one path in detail. The document shall also cover the external interfaces and internal connections. In particular, the documentation shall explain how independence is maintained between the various computer interfaces from a power supply and power loading perspective.

This design must also include a description of all programmable components in the data path and how isolation is maintained in cases where the firmware has been tampered with or the firmware has failed.

J.3 Isolation Means Justification

The documentation shall include a section that refers to each one of the unauthorized data flows listed in Annex D of this PP, how isolation is provided and how the risk is mitigated by the TOE. The details shall include a description of the method used in the TOE to assure that the specific unauthorized data flow will be blocked. The document shall also provide justification for each method used based on the threats defined in Chapter 2 of this PP.

J.4 Firmware Dependencies

Documentation shall include a section dedicated to areas in the TOE where isolation strength depends on firmware functions. This shall describe how all microcontrollers or other components handle multiple data streams coupled to multiple computers. The documentation shall describe the methods used to assure that firmware failure would not result in catastrophic TOE data isolation failure.