

# Open Trusted Computing (OpenTC)

Private Electronic Transactions (PET)

Proof of Concept prototype

Test instructions for the end user

Supported versions:

otc-dsl-pet-1.0 and otc-suse-pet-1.0.1 live CDs

## 1 Introduction

A live CD containing a proof of concept for the PET application scenario has been developed within the frame of the OpenTC project. The present test plan helps the user test the otc-suse-pet-1.0 and otc-dsl-pet-1.0 live CDs.

The user should follow the steps in the same order they are presented and report the results to the OpenTC Consortium. The user should also describe the platform he is using. At the end of the document the user can provide comments, requirements and propose further tests.

## 2 Disclaimer of warranty

The following disclaimer applies to “OpenTC PET Proof of Concept prototype” (shortly PET PoC), the object of this test plan.

**The following software: “OpenTC PET Proof of Concept prototype” is experimental and is provided “as is”, and no guarantee or warranty is given by the OpenTC consortium that the software is fit for any particular purpose. The user thereof uses the software at its sole risk and liability. The Open\_TC consortium shall have no obligation to maintain or support this software. THE Open\_TC CONSORTIUM MAKES NO EXPRESS OR IMPLIED WARRANTY OF ANY KIND REGARDING THIS SOFTWARE. The OpenTC CONSORTIUM SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, IN CONNECTION WITH OR ARISING OUT OF THE FURNISHING, PERFORMANCE OR USE OF THIS SOFTWARE.**

The Open\_TC Consortium consists of the following partners:

Technikon Forschungs- und Planungsgesellschaft mbH  
Infineon Technologies AG  
Hewlett-Packard Ltd HP UK  
IAIK, Graz University of Technology  
Lehrstuhl für Datenverarbeitung, Technische Universität München  
SUSE Linux Products GmbH  
Royal Holloway and Bedford New College  
ITAS, Forschungszentrum Karlsruhe GmbH  
TUBITAK, National Research Institute of Electronics & Cryptology  
Politecnico di Torino  
Budapest University of Technology and Economics  
Commissariat à l’Energie Atomique-LIST  
Horst Goertz Institute for IT Security, Ruhr-University Bochum  
Technische Universitaet Dresden  
University of Cambridge Computer Laboratory, University of Cambridge  
IBM Research GmbH  
Institute for Security and Open Methodologies  
Advanced Micro Devices  
Portakal Teknoloji Egitim Danismanlik Yazilim Turizm Taahhut  
INTEK  
Technical University of Sofia

Reference to the Open\_TC Consortium above shall be taken to be a reference to each discrete partner, all of whom benefit individually from the above disclaimer.

### 3 Test Strategy

This test plan covers the whole process from the boot of the platform to the remote attestation. Some steps depend on others, some steps don't. A dependency between two steps is indicated as a precondition. If a step does not depend on other steps, it can be executed at any time. Nonetheless, it is preferable to follow the proposed order.

Taking ownership of the TPM is a required operation to perform the tests defined in this plan. This is an operation with permanent effects to be executed on a TPM that has never been used and has been enabled for the first time, or after the TPM has been cleared.

**Important note: clearing the TPM is an irreversible operation that causes the loss of the keys and data previously protected by the TPM; therefore this operation *must* be done only on platforms used for testing purposes.**

**Experienced users might want to test this live CD on platforms in production that don't make use of the TPM. In so doing, these users act at their own risk. Please carefully read the "known problem" section in the README file available from the root of the CD file system.**

**No responsibility for the OpenTC consortium and the partners that contributed to this live CD for any mistaken use or damage occurred. Before starting the test procedure, the user should read the complete disclaimer of warranty provided at section 2: if the user does not agree in full about such disclaimer, he should not use the OpenTC PET Proof of Concept prototype live CD.**

Note that clearing the TPM should also result in disabling it. Therefore the user will then have to re-enable the TPM before rebooting. Clearing and re-enabling the TPM are operations to be done via the BIOS. Since the details of these operations vary from platform to platform, a detailed procedure is not provided in this document.

The remote attestation process requires a complex procedure. Should any error occur, the user must write down the problem, the output of the client proxy (see section 6.2.13) - and anything else that may be important. All these information should then be reported to the OpenTC Consortium. Should the the remote attestation fail, the user will try the procedure again and report the problem if it occurs again. Always restart the client proxy before trying again the procedure. The user can also reboot the bank domain (see section 6.2.6), but in this case he must register the platform again (see section 6.2.12) before performing the remote attestation, because the bank domain is measured every time it is started and the value of the PCR where its measurement is stored will change.

#### 3.1 Tips for experienced users

It is possible for experienced users to perform only a few tests instead of doing the whole sequence described in this plan. To help people perform these specific tests, a few tips are provided below.

- It is possible to avoid clearing the TPM and taking ownership of the TPM again if ownership has already been taken using the live CD scripts. In this case it is possible to perform the whole test plan, reboot the machine and perform again the test plan but skipping the operation of taking the ownership.

- If the user already took ownership of the platform but by means different from those provided with the live CD and he wants to avoid clearing the TPM and taking ownership again (in order not to lose all keys protected by the TPM), he will probably experience problems while performing the subsequent steps. This may be due to the Owner and Storage Root Key passwords set for the TPM that are different from the one used by the live CD scripts. The live CD assumes that the following passwords: the Owner password is

`ownerpwd`

and the Storage Root Key password is

`srkpwd`

Therefore if the user wants to keep the current ownership, he or she can avoid clearing the TPM and taking ownership again simply by modifying the passwords in the following configuration file:

`/usr/share/opentc/scripts/otc-pet-functions`

However, this procedure must be performed after every reboot since the modifications done to this file are lost after a reboot.

- Some of the steps described in the procedure are not mandatory. For instance, after ownership has been taken or the configuration file mentioned above has been modified, the test sequence becomes:

1. start the bank domain;
2. create an AIK;
3. store the AIK on a USB token;
4. restore the AIK from a USB token;
5. create the known-good values;
6. register the platform;
7. test the remote attestation.

- Even the above steps are not all mandatory. Storing (see section 6.2.9) and restoring (see section 6.2.10) the AIK to/from a USB token are optional steps: they can be performed if the user wants to use the AIK created after rebooting the machine. Each time the bank compartment is started, it is measured and a PCR is extended with the measurement. This operation changes the known-good values (see section 6.2.11) and the user must register the platform again (see section 6.2.12). If the user wants to start and stop the trusted compartment several times and perform the remote attestation without registering the platform again, he or she must disable the measurement while re-starting the compartment. This can be done by commenting the line corresponding to the measurement of the compartment in the following script:

`/usr/share/opentc/scripts/start-domT.sh`

- The user does not need to create the AIK more than once after each boot of the live CD. After the first AIK creation, the AIK is used until the system is rebooted or halted.

## 4 Prerequisites

- Test platform: a machine dedicated to testing whose TPM can be cleared without any risk of losing protected data.
- Wired network connection: WiFi, GPRS and UMTS adapters are not supported.
- DHCP server: since the tests can be performed with the platform disconnected from the network, DHCP server is optional and needed only if the tester wants to use services available on the network; if used, DHCP must be able to provide Domain-0 with the network configuration including an IPv4 address and related netmask, the default gateway and the address(es) of the DNS server(s).
- If DHCP is used, outgoing network connection (to the Internet) must be unfiltered or filtered through a *non-anonymous* HTTP proxy, if the client runs behind a firewall.

## 5 Test plan

Before starting the sequence of tests described in this test plan, the *TPM must be cleared* using the BIOS of the platform and *re-enabled*.

The OpenTC PET PoC supports two different hypervisors: Xen and L4. Each hypervisor can be tested under different configurations. This test plan is divided according to each hypervisor.

The different configurations available are:

- expert user mode: this configuration enables all the operations of the demonstrator and all the components of the OpenTC PET PoC like AIK creation, platform registration, domain management, etc.
- normal user mode: this configuration hides much of the details and provides a user-friendly interface
- good DomT mode: this configuration executes a “good” trusted domain.
- rogue DomT mode: this configuration executes a “rogue” trusted domain. In practice the rogue trusted domain differs from the good one, as if it was modified possibly due to an attack. Using the rogue domain the user can test that the trusted infrastructure prevents accessing the protected server using modified domains.

The choice of the configuration is done at boot time via the grub boot menu.

The OpenTC PET PoC provides a server domain (called domS) that is used for testing the web and proxy servers using a software TPM emulator. The IP address of the server domain is 172.31.253.2 (domSbox). The client side of the system is configured to use this server as default. The user can specify another proxy server in the following file: `/etc/otc-proxy-srv`.

## 6 Xen’s test plan

### 6.1 Test Subset 1: Normal user mode test

#### 6.1.1 Trusted GRUB detects the TPM

The TPM is detected by trusted GRUB.

Normal flow

1. The user switches on or reboots the PC with the otc-dsl-pet or the otc-suse-pet live CD in the CD/DVD drive: the system boots from the live CD
2. The user verifies if Trusted GRUB detected the TPM, that is needed for measuring the boot kernels and modules: the user checks the top-left corner of trusted GRUB menu for the string:

`TPM detected`

this message indicates that trusted GRUB successfully detected the TPM.

3. It is possible to select the layout of the keyboard by passing the parameter

`lang=xx`

to the kernel, where `xx` is the country code in small letters for the desired layout (e.g. `us`, `it`, etc).

### 6.1.2 Log In

The user logs in as `root`.

#### Normal flow

1. After the system boots, the login shell is displayed to the user:

`dom0box login:`

2. the user must type

`root`

with blank password (press enter).

### 6.1.3 X server start

The user starts the X server.

#### Normal flow

1. The user types:

`startx [resolution]`

The (optional) screen resolution can be:

- 1024x768
- 1280x1024
- 1400x1050
- 1600x1200

If no resolution is provided, the X server runs with resolution 1024x768.

DomU and DomT are then loaded automatically, this may take a few minutes depending on the platform. The user must wait until DomU and DomT are displayed.

DomU will be displayed first, then DomT will be loaded. Since DomT is measured, it may take a while between DomU and DomT are displayed. Once DomT is loaded and displayed, the user can switch between the two domains by pressing the following keys:

- ALT+F1: DomU
- ALT+F2: DomT

A few icons are available on the desktop and should be used to interact with the OTC system. The icons provided are:

- **Readme**: displays the readme.
- **Start normal mode**: starts the normal mode script. This command performs all the operations needed in order to test the remote attestation.
- **Dom0 console**: opens a console to Domain-0. This is useful for debugging operations.
- **Show log**: displays the log of the commands executed by the normal mode script.
- **Delete AIK**: deletes the AIK from the USB device, if present.
- **Reboot**: reboots the system.
- **Poweroff**: powers off the system.

Note: only one command can be started at a time.

#### 6.1.4 Normal mode start

The user starts the normal mode.

##### Normal flow

1. The user clicks on the icon

**Start normal mode**

2. A window pops up and displays the output of the process.
3. At the end of the process, ownership of the TPM is taken (if not yet taken), an AIK is created, the know-good values are created and uploaded to the bank proxy server (values are disabled), and the client proxy is started.

#### 6.1.5 Platform enabling

The user enables his platform on the bank proxy server.

##### Preconditions

- The normal mode is active (step 6.1.4).

##### Normal flow

1. The user uses a web browser (Firefox) and types the following URL:

`https://domSbox:8443/`

2. The user logs in to this website with the following credential:
  - username: `bank-op`
  - password: `otc`

3. Once successfully logged in, the user follows the link:  
`Management of the platform registration`
4. The user then follows the link to the platform `OTC-generic`.
5. The user enables the known-good values by clicking on the corresponding link.

### 6.1.6 Remote attestation test

The user tests the remote attestation process.

#### Preconditions

- The normal mode is active (step 6.1.4).
- The platform is enabled on the bank proxy server (step 6.1.5).

#### Normal flow

1. The user switches to the bank domain window (`ALT+F2`).
2. The user clicks on the Firefox toolbar bookmark named:
  - `Transp. Tunnel (domS)`
3. The user can then check the output of the client proxy by:
  - (a) switching to the DomU window (`ALT+F1`).
  - (b) clicking on the icon corresponding to the log of the system.

### 6.1.7 System stop

The user stops the system.

#### Normal flow

1. The user clicks on the icon `Dom0 console` and types `reboot` or `halt`.

## 6.2 Test Subset 2: Expert user mode test

### 6.2.1 Trusted GRUB detects the TPM

The TPM is detected by trusted GRUB.

#### Normal flow

1. The user switches on or reboots the PC with the `otc-dsl-pet` live CD in the CD/DVD drive: the system boots from the live CD
2. The user verifies if Trusted GRUB detected the TPM, that is needed for measuring the boot kernels and modules: the user checks the top-right corner of trusted GRUB menu for the string:

`TPM detected`

this message indicates that trusted GRUB successfully detected the TPM.

3. It is possible to select the layout of the keyboard by passing the parameter

`lang=xx`

to the kernel, where `xx` is the country code in small letters for the desired layout (e.g. `us`, `it`, etc).

### 6.2.2 Log In

The user logs in as `root`.

#### Normal flow

1. After the system boot, the login shell is displayed to the user:

```
box login:
```

2. the user must type

```
root
```

with blank password (press enter).

### 6.2.3 X server start

The user starts the X server.

#### Normal flow

1. The user types:

```
startx [resolution]
```

The (optional) screen resolution can be:

- 1024x768
- 1280x1024
- 1400x1050
- 1600x1200

If no resolution is provided, the X server runs with resolution 1024x768.

### 6.2.4 TPM module loading

The user checks if the TPM module is loaded. If not, the user loads it.

#### Normal flow

1. The user clicks on the icon:

```
Show loaded TPM drivers
```

2. If the TPM module is not loaded, the user must load the module.

The TPM modules available are:

- `tpm_infineon` (versions 1.1 and 1.2)
- `tpm_atmel` (version 1.1)
- `tpm_nsc` (version 1.1)
- `tpm_tis` (version 1.2)

- (a) The user can load the module by typing the following command in a shell:

```
# modprobe <tpm module name>
```

- (b) After this command is executed, the module should be loaded. The user can check if the module is present by clicking on the icon:

```
Show loaded TPM drivers
```

### 6.2.5 Vanilla domain start

The user runs the vanilla domain.

#### Preconditions

- The X server is running (step 6.2.3).

#### Normal flow

1. The user clicks on the icon:

`Start Vanilla Domain (DomU)`

2. A window pops up and displays the result of the process.
3. When the untrusted vanilla domain is ready, it appears in fullscreen.
4. The user can switch between the two domains by pressing the following keys:
  - ALT+F1: DomU
  - ALT+F4: Domain-0
5. A few utilities are provided in order to check information relative to Xen:
  - Xen Top: displays the list of running domains and their work load. The user obtains this list by clicking on the following icon:

`VMM Monitor`

- it is possible to connect to the console of the vanilla domain (called DomU). If this is done during DomU's boot process, the output of the boot is displayed to the user. If the user wants to connect to the DomU console, he clicks on the icon:

`Vanilla Domain Console (DomU)`

### 6.2.6 Bank domain start

The user runs the bank domain. Note that this process modifies the values of the PCRs (unless the starting script is modified, see section 2.1). It is useful to list the values of the PCRs before and after having executed this task to check what happened.

#### Preconditions

- The X server is running (step 6.2.3).

#### Normal flow

1. If the user wants to display the values of the PCRs, he clicks on the icon:

`Show PCR values`

2. The user clicks on the icon:

`Start Bank Domain (DomT)`

3. A window pops up and displays the result of the process.
4. When the bank domain is ready, it appears in fullscreen.

5. The user can switch between the two domains by pressing the following keys:
  - ALT+F2: DomT
  - ALT+F4: Domain-0
6. If the user wants to see how the values of the PCRs are changed, he must click on the icon:

Show PCR values

7. A few utilities are provided in order to check information relative to Xen:
  - Xen Top: displays the list of running domains and their work load. The user obtains this list by clicking on the following icon:  
VMM Monitor
  - it is possible to connect to the console of the trusted domain (called DomT). If done during DomT's boot process, the output of the boot is displayed to the user. If the user wants to connect to the DomT console, he clicks on the icon:  
Bank Domain Console (DomT)

### 6.2.7 Taking ownership of the TPM

The user takes ownership of the TPM if it is not yet taken. Using this live CD ownership should only be taken once, unless the TPM is cleared or the passwords for ownership or the Storage Root Key (SRK) are different from the default ones. Rebooting the machine for performing another sequence of tests doesn't require taking ownership again.

#### Preconditions

- The TPM is enabled.
- Ownership of the TPM has not yet been taken after having cleared the TPM.
- The module with the TPM driver is loaded (step 6.2.4).

#### Normal flow

1. The user clicks on the icon:

Take TPM's Ownership

2. A window pops up and displays the output of the process.
3. At the end of this process the user has taken ownership of the TPM.

### 6.2.8 AIK Creation

The user creates an Attestation Identity Key (AIK). This procedure will create an AIK and the related X.509 certificate and will then activate the new identity.

#### Preconditions

- The module with the TPM driver is loaded (step 6.2.4).
- The user has taken ownership of the TPM (step 6.2.7).

#### Normal flow

1. The user clicks on the icon:

`Create AIK`

2. A window pops up and displays the output of the process.
3. The user is asked to enter the platform name. He can choose a new name or use the default one (`OTC-generic`).
4. At the end of this process the system updates the file:

`/usr/share/opentc/iaik-proxy/config/client.ini`

in order to be able to use the new AIK.

### **6.2.9 AIK storage on USB token**

The user can store the AIK on a USB token in order to use it later. This procedure creates a directory called `OpenTC` on the USB token and stores the AIK in that directory. This procedure is useful if the user wants to reboot the machine and test the system with the previously created AIK.

#### Preconditions

- An AIK has been created (step 6.2.8).
- The user connected a USB token.

#### Normal flow

1. In order to store the AIK on the USB token, the user clicks on the icon:

`Store AIK data on USB token.`

2. A window pops up and displays the output of the process.
3. The system checks if a USB token is present. If it is present, the system asks the user if he wants to use that token to store the AIK data.
4. At the end of this process the system creates the directory `OpenTC` on the USB token and copies the AIK and the related data to that directory

### **6.2.10 Restore AIK from a USB token**

The user can restore the AIK data previously stored on a USB storage. This procedure backs up the current data and restores the data from the USB storage.

#### Preconditions

- An AIK is stored on a USB token (step 6.2.9).
- The user connected a USB token.

#### Normal flow

1. In order to restore the AIK from the USB token, the user clicks on the icon:

`Restore AIK data on USB token.`

2. A window pops up and displays the output of the process.
3. The system checks if a USB token is present. If it is present, the system asks the user if he wants to use that token to restore the AIK data.
4. The system checks if the directory `/usr/share/opentc/.psbackup` exists.

If the directory does not exist, the system creates the directory and use it to back up the current AIK data, and then restores the AIK data from the USB token.

If the directory exists, the system notifies the user and does not restore the AIK and the related data from the USB token.

If the directory exists and the user wants to restore the AIK from the USB token, he must remove the directory following the below steps:

- (a) Click on the ATerminal icon
- (b) Type `rm -rf /usr/share/opentc/.psbackup`

### 6.2.11 Known-good values creation

The user creates a set of known-good values.

#### Preconditions

- The module with the TPM driver is loaded (step 6.2.4).

#### Normal flow

1. The user clicks on the icon:

`Register Platform`

2. A window pops up and displays the output of the process.
3. A file with the known-good values is created. The file name and the related pathname are displayed at the end of the process.
4. Note that the set of known-good values is the digest of the values of all PCRs - including the PCR extended when the bank domain is started. If, for any reason, the user stops the bank domain and starts it again, he must create another set of known-good values and register the platform again.

### 6.2.12 Platform registration

The user registers his platform to the bank proxy server.

#### Preconditions

- An AIK has been created (step 6.2.8).
- The known-good values have been created (step 6.2.11).

#### Normal flow

1. The user uses a web browser (Firefox) and types the following URL:

`https://domSbox:8443/`

If the test client is behind a firewall and the server is not DomS, the browser must be configured to use a HTTP proxy for connecting to the Internet.

2. The user logs in using the following credential:
  - username: `bank-op`
  - password: `otc`
3. Once successfully logged in, the user follows the link:
 

`Management of the platform registration`
4. If there is not yet a platform with the name the user gave to his platform, the user registers a new platform by clicking on the corresponding link.
5. The user then follows the link corresponding to his platform.
6. The user finally uploads the file with the known-good values by clicking on the corresponding link.

### 6.2.13 Client proxy start

The user runs the client proxy.

#### Preconditions

- An AIK has been created (step 6.2.8).
- The platform is registered (step 6.2.12).

#### Normal flow

1. The user clicks on the icon:
 

`Start Client Proxy`
2. A window pops up and displays the output of the process.
3. The current configuration for the HTTP proxy (e.g. when the test client is behind a firewall) will be shown; during the first run of the proxy after the boot of the system, no HTTP proxy is configured.
4. The user is asked to choose one of the following options:
  - confirm the current configuration by pressing `<enter>`
  - set a new HTTP proxy by typing
 

`<IP address>:<TCP port><enter>`

or

`<hostname>:<TCP port><enter>`
  - force the client proxy not to use any HTTP proxy by typing
 

`NONE<enter>`
5. *NOTE: the use of an HTTP proxy is not needed with this version of the Proof of Concept prototype.* When the proxy is ready, it outputs the message:
 

`Init complete`
6. The user must not close this window. If he closes this window, the client proxy is stopped.
7. The client proxy window displays the output of the client proxy during the remote attestation process.

#### 6.2.14 Remote attestation test

The user tests the remote attestation process.

##### Preconditions

- The bank domain is running (step 6.2.6).
- The platform is registered and enabled to the bank proxy server (step 6.2.12).

##### Normal flow

1. The user switches to the bank domain (ALT+F2).
2. The user clicks on the Firefox toolbar bookmark named:
  - Transp. Tunnel (DomS)
3. The user can then check the output of the client proxy by:
  - (a) switching to Domain-0 (ALT+F4).
  - (b) focusing on the window of the client proxy.

#### 6.2.15 Bank domain stop

The user stops the bank domain before shutting down the machine.

##### Preconditions

- The bank domain is running (step 6.2.6).

##### Normal flow

1. The user switches to Domain-0 (ALT+F4).
2. The user clicks on the icon:

Stop Bank Domain (DomT)
3. A window pops up and displays the result of the process.

#### 6.2.16 Vanilla domain stop

The user stops the vanilla domain before shutting down the machine.

##### Preconditions

- The vanilla domain is running (step 6.2.5).

##### Normal flow

1. The user switches to Domain-0 (ALT+F4).
2. The user clicks on the icon:

Stop Vanilla Domain (DomU)
3. A window pops up and displays the result of the process.

### 6.2.17 System stop

The user stops the client proxy before shutting down the system.

#### Preconditions

- The bank domain is stopped (step 6.2.15).
- The vanilla domain is stopped (step 6.2.16).

#### Normal flow

1. The user stops the client proxy by:
  - (a) focusing on the window that displays the output of the client proxy.
  - (b) pressing the keys CTRL+C.
2. The user can now safely shut down the platform.

## 7 L4's test plan

Testing the system with the L4 supervisor is very similar to testing it using the Xen hypervisor. The only differences are related to the boot menu, the keyboard layout selection and how to switch between the domains.

### 7.1 Supported TPM

Under L4, only TPMs version 1.2 are supported.

### 7.2 Boot menu

The configuration offered by the OpenTC PET PoC with L4 are:

- expert mode, good, advanced
- expert mode, rogue, advanced
- normal mode, good, advanced

### 7.3 Keyboard layout selection

It is not possible to specify at boot the keyboard layout with L4. It is only possible to change the keyboard layout on a version of the demonstrator installed on the hard disk. (For HD installation only, when available: once installed, if the user wants to change the keyboard layout, he must edit the files `/l4/etc/dom*.cfg`).

#### 7.3.1 Switching between the domains

L4 uses a MicroGUI interface to display the domains. The MicroGUI has two different modes: thumbnails and fullscreen.

In the thumbnail mode, a thumbnail of all the domains is shown on the screen. In the fullscreen mode, only the selected domain is shown in fullscreen. Switching between the thumbnail mode and the fullscreen mode is obtained by pressing the F12 key.

When in the thumbnail mode, domains are selected using the arrow keys and the selected domain is switched to fullscreen mode by pressing the Enter key.

When in the fullscreen mode, it is possible to switch between the domains by pressing on the keys ALT+PageUP and ALT+PageDown.

## 7.4 Xen-only commands

Commands like VMM monitor, Bank Domain Console (DomT) or Stop Vanilla Domain (DomU) work only under Xen.