Open Source TPM support

Open source application and support software for TPM is available for several operating systems like Linux, Android and in different programming languages supporting the following scenarios:

- embedded Systems
- servers
- mobile communication and portable devices (e.g. tablet computer or smartphone)

Open source implementations can also be ported to other platforms and processors and may be act as a starting point for the development of new applications. Some open source projects from the following list are supported by Infineon while other packages are separately developed by independent parties. The following list of Open Source software utilizing Trusted Computing and/or TPM software makes no claim to be complete and represents a limited number of projects:

1. **Linux TPM Driver** (http://www.kernel.org)
   Linux device driver for Trusted Platform Modules (TPM) in standard kernel (Vanilla).

2. **I2C driver for TPM**
   The driver is available on Linux kernel.org (https://lkml.org/lkml/2011/7/22/137)

3. **Trusted GRUB** (http://sourceforge.net/projects/trustedgrub)
   Trusted GRUB extends the GRUB bootloader for Linux platforms with TPM support. This makes it possible to provide a secure Bootstrap architecture; Code is in general useful for initializing a Trusted Platform Module and execute integrity measurement based on Trusted Computing.

4. **UBoot based on TPM with I2C**
   (http://git.chromium.org/gitweb/?p=chromiumos/third_party/u-boot.git;a=tree;f=drivers/tpm/slb9635_i2c;hb=chromeos-v2011.03)
   UBoot involving TPM using I2C interface.

5. **The TROUSERS project** (http://sourceforge.net/projects/trousers):
   An open-source TCG Software Stack implementation created and released by IBM. TROUSERS is concentrating on an implementation of the TCG TSS-stack for Linux, using the C programming language.

6. **API modules for trusted computing** (ibmswtpm.sourceforge.net)
   Several software packages esp. libtpm as low level library for embedded applications.

7. **The Trusted JAVA project** (http://trustedjava.sourceforge.net/)
   It shows how JAVA can use the functions of a TPM and the TSS stack for increasing the trust level. Several implementations are available.

8. **TPM/J Project** (http://tpmj.sourceforge.net)
   Java-based API for the Trusted Platform Module (TPM), also useful for Android OS. It is not compatible to the TSS specification

9. **TrouSerS ported to Windows**
   (http://security.polito.it/trusted-computing/trousers-for-windows/)
   It is a port of the Trousers TSS Stack for the Windows operating system.

10. **OS independent implementation of the Trusted Network Connect (TNC) specification from Trusted Computing Group (TCG)**
    (http://sourceforge.net/projects/libtnc)
    Functions for loading and communicating with TNC plugins, sample IMC and IMV plugins, TNCCS-XML support on Windows, Linux, Mac, *BSD.

11. **Linux Integrity Subsystem** (http://linux-ima.sourceforge.net/)
    This was introduced in Linux Kernel 2.6.30. The Integrity Subsystem of the kernel allows detecting if files have been accidentally or maliciously modified.

12. **Open Platform Trust Services** (http://sourceforge.jp/projects/openpts/)
    An Open-Source implementation of the Platform Trust Services (PTS).

For further information do not hesitate to contact us: *tpm-support@infineon.com*