Device insertion and removal robustness: The device may be inserted and removed at any time (including device boot, mid-transaction, or conclusion of transaction session) without adversely affecting either the host PC, or the device itself.

As per the above requirements, Figure 4 shows our high-level reference design of a USB-based TCG containing a TCG Trusted Platform Module (TPM). The most notable difference between our reference platform to that of TCG PC reference platform [8] is that (1) the device does not have any user input or output devices such as a display or keyboard and (2) there is only a single physical network interface to the device, namely the USB port.

Our goal was to achieve a hardware implementation that stays as close as possible to the reference platform shown in Figure 4. Our aim was to show the feasibility of the idea through the development of a concept demonstrator. Given the time to develop, integrate and test the hard and software systems, it was decided very early in the project to base the implementation on an existing embedded hardware platform. We investigated various embedded systems using the following criteria: good support for a version of the Linux operating system; development tools that allow easy development; a USB form factor and a significant community of users and developers. These criteria lead us to the select of the Gumstix Overo Earth Computer-on-Module (COM) [42]. The development kit associated with this product features a motherboard that carries the Gumstix Overo Earth COM as a daughterboard, and offers a rich variety of interfaces: a USB OTG port, two mini USB serial (terminal) ports, control and status ports and some forty general purpose input/output ports that can used for a variety of uses, including interfacing to the TPM chip and providing clock and data input and output.

Using this development kit allowed us to quickly prototype a secondary “TPM only” board that connected to the development kit motherboard, and allowed the software development to progress without waiting for the final design and implementation of a small, USB form-factor motherboard.

Figure 5 shows the implementation hardware architecture for the proposed device. As mentioned above, the device replaced the development kit and attached secondary prototype “TPM only” boards with a single, USB-form factor motherboard, that connects the Gumstix Overo Earth COM via two 70-way low profile AVX connectors. The motherboard carries the TPM chip, clock generation, voltage regulators and logic level conversion (to allow interfacing between 1.8 V, 3.3V and 5V logic levels) circuitry, a USB plug with input protection circuitry and two low profile 70 pin EVX sockets. Figure 6 shows the completed hardware device, as viewed from the component side of the motherboard. Given that the implemented device has no (usual) user interface, the motherboard design included two status information LEDs, one indicating that the system has power, and the other that the device has successfully booted.

The motherboard components are divided into two major subsystems: the TPM subsystem and power supply subsystem.

The TPM subsystem consists of the TPM chip itself, logic level shift circuitry to interface the TPM chip’s 3.3V logic to the Overo Earth COM 1.8V logic, a TPM reset circuit and a timing oscillator for the TPM chip.

The selection and sourcing of the TPM chip was somewhat unusual, as the system implementation was on a commercial embedded computer, rather than a general purpose PC. This meant that there were restrictions on the type of TPM chip that could be used. Most of the widely available TPM chips are meant to be integrated into a general purpose PC (whether it be laptop or desktop), and connected via the PC’s own internal LPC bus [43]. Unfortunately, commercial embedded computers do not use this bus to interconnect the various devices found on a embedded computing platform. They do however offer a large number of serial (GPIO) [44] interfaces and that in turn meant that the design had to rely on a serial bus version of a TPM chip – the Atmel