

# Master-IT: Project work WS2010/2011

## Topic: Integration of a Trusted Platform Module (TPM) into a NIOS II system

**Area: IT Security, SW Development**

Start: October 2010  
Partner: Internal project  
Tools: Altera Quartus II  
Prerequisites: Programming know-how in VHDL / C

### Description

Trusted Platform Modules (TPM) are mainly integrated in Office PCs. The interface used with a PC (LPC) is not suited for use in small embedded devices like the NIOS II platform. But there also exists a TPM with an I<sup>2</sup>C interface which might be a good option to be used with embedded platforms.

### Goal

The Goal of this Project is to connect a TPM with an I<sup>2</sup>C-Interface with a NIOS II development board. In particular, in carrying out this project work you should

- learn TPM basics,
- integrate an I<sup>2</sup>C IP-core in Altera's NIOS II system,
- develop a basic software module to test the communication with the TPM.

Contact: Prof. Dr. Stefan Heiss [stefan.heiss@hs-owl.de](mailto:stefan.heiss@hs-owl.de) (Supervisor)  
M.Sc. Stefan Hausmann [stefan.hausmann@hs-owl.de](mailto:stefan.hausmann@hs-owl.de)