Atmel Trusted Platform Module (TPM) Devices

Atmel® Trusted Platform Module (TPM) devices provide strong hardware-based public key (RSA) security for personal computers and embedded processors on a single chip. Atmel TPM devices are complete turnkey systems that integrate three industry-leading Atmel IP: Atmel AVR® microcontrollers, Atmel EEPROMs, and Atmel security technologies. The devices support secure boot via platform integrity measurements, intellectual property protection, authentication, and secure communications.

Atmel TPM Kits

Atmel Trusted Platform Module Development kits are custom USB-based development boards based on the Atmel SAM4S ARM®-based microcontroller and Atmel TPM devices. User-friendly demonstration and evaluation software is provided on a USB Flash drive. The drive contains demonstration source code, hex images for reloading the demo code (if necessary), and kit schematics. A USB extension cable is also included. The kit is updateable with the latest firmware, whenever available.
<table>
<thead>
<tr>
<th>Name &amp; Ordering Code</th>
<th>Function</th>
<th>Detailed Description</th>
<th>Kit Contents</th>
</tr>
</thead>
</table>
| AT97SC3205T-SDK2    | Development Kit for AT97SC3205T I2C TPM Device | Custom USB-based development board based on the Atmel SAM4S ARM microcontroller and Atmel AT97SC3205T TPM device with I2C interface. User-friendly demonstration and evaluation software is provided on a USB Flash drive. The drive contains demonstration source code, hex images for reloading the demo code (if necessary), and kit schematics. A USB extension cable is also included. The kit is updateable with the latest firmware, whenever available. (Please contact crypto@atmel.com for more details on demonstration software updates.) | • AT97SC3205T I2C TPM board (TCG v1.2)  
• USB extension cable  
• USB Flash drive |
| AT97SC3205P-SDK2    | Development Kit for AT97SC3205P SPI TPM Device | Custom USB-based development board based on the Atmel SAM4S ARM microcontroller and Atmel AT97SC3205P TPM device with SPI interface. User-friendly demonstration and evaluation software is provided on a USB Flash drive. The drive contains demonstration source code, hex images for reloading the demo code (if necessary), and kit schematics. A USB extension cable is also included. The kit is updateable with the latest firmware, whenever available. (Please contact crypto@atmel.com for more details on demonstration software updates.) | • AT97SC3205P SPI TPM board (TCG v1.2)  
• USB extension cable  
• USB Flash drive |