TN0891
Technical note

Trusted Platform Module (TPM) certificates

Introduction

STMicroelectronics embeds EK certificates (TCG Endorsement Key Credential) in its Trusted Platform Module (TPM) products.

STMicroelectronics operates its own Certificate Authority (CA) which was certified by GlobalSign®.

Several intermediate certificate authorities may be created in order to discriminate different application major revisions or product technology. The following table defines the current link between intermediate CAs and product sales types.

Table 1. Intermediate CAs and TPM products (as of January 2012)

Certificate Authority	Part number	Ordering code
ST Intermediate CA 01	ST19NP18-TPM	ST19NP18ExxxPVMT ST19NP18ExxxPVMK ST19NP18ExxxPVMO
ST Intermediate CA 02	ST33TPM12LPC	ST33ZP24AxxxPVSC ST33ZP24AxxxPVSH
	ST33TPM1212C	ST33ZP24AxxxPVSK
	ST33TPM12SPI	ST33ZP24AxxxPVSL

The following TPM certificates are included in the attached ZIP file:

- GlobalSign Trusted Computing CA
- ST TPM Root certificate
- ST Intermediate CA 01
- ST Intermediate CA 02
- Sample TPM EK certificate for ST19NP18PVMT (certified by ST Intermediate CA 01)
- Sample TPM EK certificate for ST33ZP24PVSC (certified by ST Intermediate CA 02)

STMicroelectronics CA infrastructure has been successfully audited by GlobalSign®. The details of the infrastructure are available in the Certificate Practice Statement.

Revision history

Table 2. Document revision history

Date	Revision	Changes
30-Mar-2012	1	Initial release.