



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. |

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST's terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY TWO AUTHORIZED ST REPRESENTATIVES, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER'S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2012 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com