life.augmented

Kerkey

Security Module for Smartgrid applications

Data brief

VQFN32

Features

- Protection profile for the Security Module of a Smart Meter Gateway (Security Module PP)
- ECC support for NIST-P-256
- Digital signature generation and verification with ECDSA
- Key agreement with Diffie-Hellman (ECKA-ECDH) and El Gamal (ECKA-EG)
- PACE with ECDH-GM-AES-CBC-CMAC-128 for secure messaging
- On-chip ECC key pair generation
- ISO7816-4 file system with EFs, DFs and ADFs, including nesting of DFs
- Key pair, public key and PIN objects
- Extended length APDUs
- ECOPACK® 32-lead VFQFPN 5x5 mm (0.5 mm pitch)

Platform

- Java Card™ inside (Version 2.2)
- GlobalPlatform™ (Version 2.1.1)
- ISO/IEC 7816 T=0 and T=1 contact protocols
- Common personalization specification (CPS) compliant

Hardware

- Enhanced 8/16-bit ST23 CPU core with 16 Mbytes linear addressable memory
- 80 Kbytes of User EEPROM including 128 bytes of User OTP area:
  - 30-year data retention at 25° C
  - 500,000 erase/write cycles at 25° C
  - 1 to 64 bytes Erase or Program in 1.5 ms
- Operating temperature: –25° to +85° C
- Enhanced NESCRYPT crypto-processor for public key cryptography
- Hardware security enhanced DES accelerator
- Contact assignment compatible with ISO/IEC 7816-3 standards
- Asynchronous receiver transmitter (IART) for high speed serial data support (ISO/IEC 7816-3 and EMV™ compliant)
- ESD protection greater then 6 kV (HBM)
- 3V and 5V supply voltage ranges
- EMVCo / CC (EAL6+) certification

Security

- AIS-31 class P2 compliant true random number generator (TRNG)
- Enhanced cryptographic algorithms:
  - DES/3DES, RSA, ECC and AES
  - SEED, SHA-1, SHA-256, MD5 and CRC16
  - Password Authenticated Connection Establishment (PACE) protocol
- Differential power analysis (DPA) and differential fault analysis (DFA) countermeasures against side channel attacks
- Active shield
- ISO 3309 CRC calculation block
- Memory protection unit (MPU)
- Unique serial number on each die

Applications

- Security module for smart metering applications

Certifications

- Product Candidate for:
  - Certification-ID BSI-CC-PP-0077
  - TR-03109-2

1 Description

The Kerkey device implements the commands defined by the BSI for the Security Module of a Smart Meter Gateway as well as Global Platform v2.1.1 commands.

Smart metering system

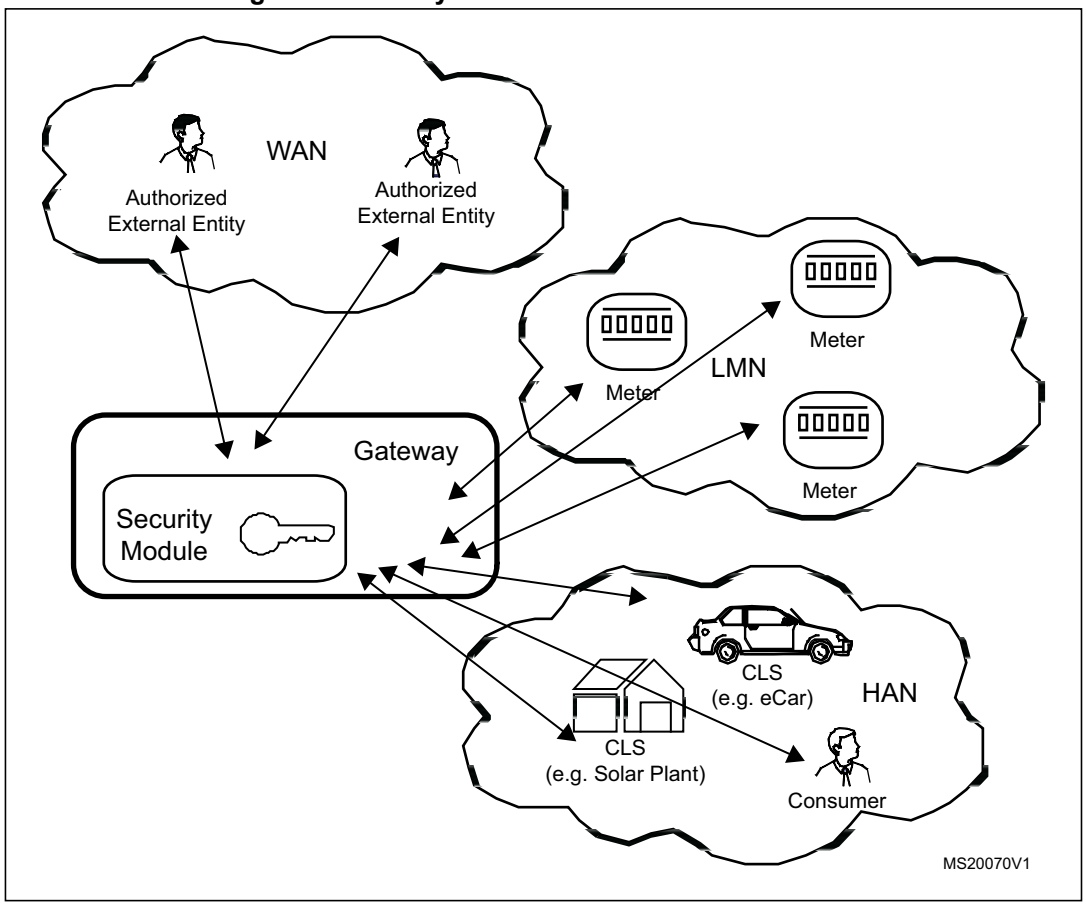
A Smart Metering System comprises the following functional units:

- The **Gateway** serves as the communication component between the components in the LAN of the consumer and the outside world. It can be seen as a special kind of firewall dedicated to the Smart Metering functionality. It also collects, processes and stores the records from Meter(s) and ensures that only authorised parties in a Wide Area Network (WAN) have access to them or derivatives thereof. Before sending relevant information the information will be signed and encrypted using the services of the Security Module (SM). The Gateway features a mandatory user interface, enabling authorised consumers to access the data relevant to them.
- The **Meter** itself is part of a Local Metrological Network (LMN) and records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) in defined intervals and submits those records to the Gateway. The Meter Data has to be signed before transfer in order to ensure their authenticity and integrity. The Meter is comparable to a classical meter[(a)] and has comparable security requirements; it must be sealed according to regulations. The Meter further supports the encryption of its connection to the Gateway[(b)].
- The Gateway utilises the services of a **Security Module** as a cryptographic service provider for different cryptographic functionalities based on elliptic curve cryptography as the generation and verification of digital signatures and key agreement which is used by the Gateway in the framework of TLS, content data signature and content data encryption. The Security Module contains the cryptographic identity of the Gateway, and it serves as a reliable source for random numbers as well as a secure storage for cryptographic keys and certificates. The Security Module is addressed within this Protection Profile. It is embedded into the Gateway and directly communicates with the Gateway.
- **Controllable Local Systems** (CLS) may range from local power generation plants, controllable loads such as air condition and intelligent household appliances (“white goods”) to home automation applications in a Home Area Network (HAN). CLS may utilise the services of the Gateway for communication services.

a. In this context, a classical meter denotes a meter without a communication channel, i.e. whose values have to be read out locally.

b. It should be noted that it is not implied that the connection is cable based.

Figure 1. Security Module and its Direct Environment



Development tools

ST provides a complete toolkit with an easy-to-use interface to manage Key and PIN objects.

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
04-Oct-2013	1	Initial release.
07-Nov-2013	2	Updated logo information on page 2.

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.

ST PRODUCTS ARE NOT DESIGNED OR AUTHORIZED FOR USE IN: (A) SAFETY CRITICAL APPLICATIONS SUCH AS LIFE SUPPORTING, ACTIVE IMPLANTED DEVICES OR SYSTEMS WITH PRODUCT FUNCTIONAL SAFETY REQUIREMENTS; (B) AERONAUTIC APPLICATIONS; (C) AUTOMOTIVE APPLICATIONS OR ENVIRONMENTS, AND/OR (D) AEROSPACE APPLICATIONS OR ENVIRONMENTS. WHERE ST PRODUCTS ARE NOT DESIGNED FOR SUCH USE, THE PURCHASER SHALL USE PRODUCTS AT PURCHASER’S SOLE RISK, EVEN IF ST HAS BEEN INFORMED IN WRITING OF SUCH USAGE, UNLESS A PRODUCT IS EXPRESSLY DESIGNATED BY ST AS BEING INTENDED FOR “AUTOMOTIVE, AUTOMOTIVE SAFETY OR MEDICAL” INDUSTRY DOMAINS ACCORDING TO ST PRODUCT DESIGN SPECIFICATIONS. PRODUCTS FORMALLY ESCC, QML OR JAN QUALIFIED ARE DEEMED SUITABLE FOR USE IN AEROSPACE BY THE CORRESPONDING GOVERNMENTAL AGENCY.

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.

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