Security module of a smart meter gateway as defined by the BSI

Features

- Product loaded with an applet compliant with the features defined by the BSI (Bundesamt für Sicherheit in der Informationstechnik, that is, the German Federal Office for Information Security) for the security module of a smart meter gateway
- Product compliant with the BSI-DSZ-CC-1037-2018 protection profile (PP): "Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)"
- Elliptic curve cryptography (ECC) support for NIST curves P-256 and P-384, and Brainpool curves P-256r1, P-384r1 and P-512r1, other curves supported depending on the product
- Digital signature generation and verification with an elliptic curve digital signature algorithm (ECDSA)
- Key agreement with Diffie-Hellman (elliptic curve key agreement algorithm (ECKA) – elliptic curve Diffie–Hellman (ECDH))
- Unwrapping of COSEM CC-LAN (local area network) and PLC-G3 pre-shared keys (PSKs)
- Password authenticated connection establishment (PACE) with ECDH-GM-AES-CBC-CMAC- 128/192/256 for secure messaging
- On-chip ECC key pair generation
- ISO 7816-4 file system with elementary files (EFs), dedicated files (DFs) and application dedicated files (ADFs), including nesting of DFs
- Key pair, public key and PIN (personal identification number) objects
- Up to 80 Kbytes of user memory
- Extended-length application protocol data units (APDUs)
- In-house personalization services
- Full ecosystem with expansion board and middleware

Platform

- Java Card™ 3.0.4 Classic Edition
- GlobalPlatform® 2.1.1
- Common Personalization Specification (CPS) compliant
- ISO/IEC 7816 T=1 contact protocols
- Standard I²C communication up to 100 kHz
- Java Card™ platform Common Criteria (CC) certification EAL5+

Hardware

- Arm® SecurCore® SC000™ 32-bit RISC core
  - 30-year data retention at 25 °C
  - 500 000 erase/write cycles at 25 °C
- Operating temperature: −40 to +85 °C
- Enhanced NESCRIPT cryptoprocessor for public key cryptography
- 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® compliance)
• Electrostatic discharge (ESD) protection greater than 6 kV (human body model – HBM) for contacts pads
• 1.62 V to 5.5 V supply voltage
• Common Criteria (EAL5+) certification
• ECOPACK® 32-lead VFQFPN 5×5 mm (0.5 mm pitch)

Security
• AIS-31 class PTG.2 compliant true random number generator (TRNG)
• AIS-20/31 class DRG.3 deterministic number generator (DRNG)
• Enhanced cryptographic algorithms:
  – DES/3DES, ECC and AES
  – SHA-1, SHA-256, MD5 and CRC16
  – Generic mapping primitive for the PACE protocol
• Hardware security enhanced DES accelerator
• Hardware security enhanced AES
• Differential power analysis (DPA) and differential fault analysis (DFA) countermeasures against side-channel attacks
• Active shield
• Unique serial number on each die

Certification
• Hardware IC Common Criteria certified EAL5+
• Java Card Platform Common Criteria certification EAL5+ (AVA_VAN.5, ALC_DVS.2)
  – Reference PP: Java Card Closed Protection Profile, v3.0
• Certified Common Criteria certification EAL4+ (AVA_VAN.5, ALC_DVS.2) for Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)
  – Reference BSI-DSZ-CC-1037-2018

Application
• Java Card/GlobalPlatform secure element providing authentication, data management and cryptographic services.
• Product loaded with an applet that provides the features defined by the BSI for the security module of a smart meter gateway.
1 Description

The STSAFE-J100-BS device implements the commands defined by the BSI for the security module of a smart meter gateway as well as the GlobalPlatform v2.1.1 commands.

A smart metering system comprises the following functional units: a gateway, meters, a security module and a controllable local system (CLS).

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 the meters and ensures that only authorized parties in a wide area network (WAN) have access to them.

Before relevant information is sent, it is signed and encrypted using the services of the security module (SM). The gateway features a mandatory user interface, enabling authorized 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 (such as electricity, gas, water or heat) in defined intervals, and submits those records to the gateway. The meter data have to be signed before transfer in order to ensure their authenticity and integrity. The meter is comparable to a classical meter and has comparable security requirements; it must be sealed according to regulations. The meter further supports the encryption of its connection to the gateway.

The gateway utilizes the services of a security module as a cryptographic service provider for different cryptographic functions based on elliptic curve cryptography. These functions include the generation and verification of digital signatures and of the key agreement, which is used by the gateway in the framework of transport layer security (TLS). The security module also provides a content data signature and content data encryption functionality. It contains the cryptographic identity of the gateway, and 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 it.

The controllable local system may range from local power generation plants, controllable loads such as air conditioning or intelligent household appliances, to home automation applications in a home area network (HAN). The CLS may utilize the services of the gateway for communication services.

The STSAFE-J100-BS is based on an Arm® core.

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.
Development tools

ST provides a complete set of tools for the integration of the security module: the STSAFE-J100-BS test tools and a development board (STS-J-PROGQ32BSI).

Note: Contact your local ST support office for available host software and drivers.
### Table 1. Document revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>07-Jun-2018</td>
<td>1</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>