AuKey

AuKey for brand protection state-of-the-art security for peripheral authentication

Data brief

SO8N
4 x 5 mm

Features

Key functions

- Peripheral authentication
- Secure data read/write from/to peripheral
- Secure counters
- Configurable key management
- Customizable security architecture
- Configurable memory partitioning

Security

- Latest generation of STMicroelectronics highly secure ST23 MCUs
  - Active shield
  - Monitoring of environmental parameters
  - Protection mechanism against faults
  - Unique serial number on each die
- Advanced cryptography
  - AES (Advanced Encryption Standard) for symmetric architecture
  - RSA (Rivest, Shamir and Adleman) or ECC (elliptic curve) for asymmetric architecture
- Secure operating system
  - Secure Aukey kernel for authentication and data management
  - Life cycle management and secure personalization
  - Protection against logical and physical attacks

Hardware

- Highly secure ST23 MCU platform
- 1 to 18 Kbyte configurable non-volatile memory
  - Highly reliable CMOS EEPROM submicron technology
  - 10 years data retention
  - 500,000 erase / program cycles endurance typical at 25 °C
  - 1 to 32 bytes erase / program in 1.5 ms
  - 3 to 5 V supply voltage range

Protocol

- I²C serial interface
  - 100 kbit/s transmission speed
  - Up to 128 peripherals on single bus

Package

- ECOPACK® SO8N 8-lead plastic small outline

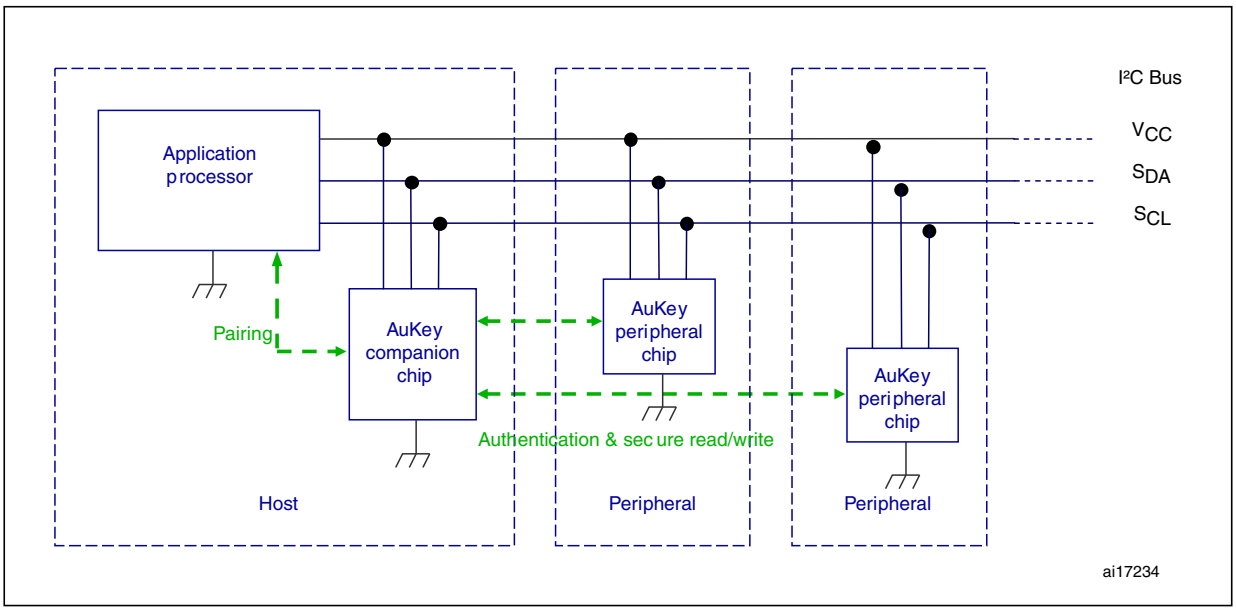
1 Description

1.1 Architecture

AuKey is a highly advanced flexible security architecture supporting symmetric and asymmetric cryptography. It is implemented as a secure operating system running on the latest generation secure microcontrollers and providing authentication and secure data management services to the host application processor.

Symmetric cryptographic architecture

Figure 1. AuKey symmetric cryptographic architecture



The symmetric architecture (*Figure 1*) uses one AuKey secure microcontroller per peripheral, and an AuKey secure microcontroller on the host main board. Symmetric cryptography (AES) allows to authenticate and authorize access to AuKey peripheral chips. It is also used for the secure channel between the host application processor and the AuKey companion chip (optional pairing), and for an optional secure channel between the equipment manufacturer remote server and the AuKey companion chip. This optional channel may be used for application processor firmware upgrade.

LICENSED DPA COUNTERMEASURES™

The symmetric cryptographic architecture supports the following features:

- Authentication

  Authentication serves to provide proof to a device application processor that a certain peripheral is genuine. This allows an equipment manufacturer to ensure that only authentic peripherals, accessories or consumables can be used in conjunction with the original equipment. The application processor authenticates the AuKey peripheral chip with the help of the companion chip through a challenge-response protocol based on AES.

- Secure read/write

  Secure write operations allow the application processor to write usage or traceability data to one of its peripherals so that it cannot be tampered with by unauthorized users.

  Secure read operations allow the application processor to authenticate the data read from the AuKey peripheral chip with the help of the AuKey companion chip. This ensures that a peripheral or an accessory is used only as intended and within the limitations defined by the equipment manufacturer.

- Secure one-way counters

  Secure one-way counters limit the usage of a certain accessories or consumable to a value preset by the manufacturer. A secure one-way counter can only be decremented.

- Early pairing to application processor (optional)

  Pairing during the production process between the AuKey cryptographic chip and the application processor on the equipment main board enables the application processor to authenticate the cryptographic chip.

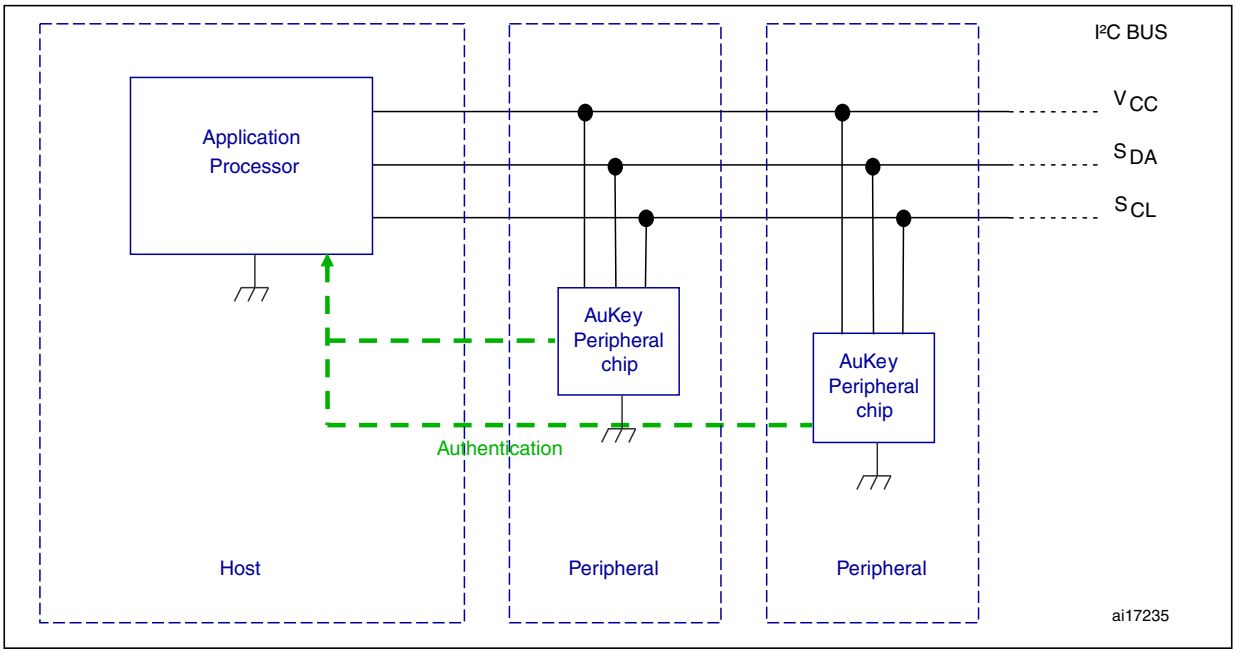
- Firmware upgrade and equipment authentication (optional)

  When the host is connected to a remote server, the AuKey companion chip provides the host manufacturer the capability to secure the upgrade of the application processor firmware or parameters. This contributes to ensure the integrity of the host, and to prevent unauthorized downloading of software. By using the AuKey companion chip for decryption, the remote download can also be encrypted by the remote server. The equipment manufacturer's server can also perform the remote authentication of the host using the AuKey companion chip.

Asymmetric cryptographic architecture

The asymmetric architecture (*Figure 2*) uses one AuKey secure microcontroller per peripheral and does not require any companion chip on the host main board. Asymmetric cryptography (RSA or ECC) allows to authenticate AuKey peripheral chips.

Figure 2. AuKey asymmetric cryptographic architecture



The asymmetric cryptographic architecture supports the following features:

- Authentication

  Authentication serves to provide proof to a device application processor that a certain peripheral is genuine. This allows an equipment manufacturer to ensure that only authentic peripherals, accessories or consumables can be used in conjunction with the original equipment. The application processor requests the AuKey peripheral chip to generate a signature over a challenge using asymmetric cryptography.

- Secure one-way counters

  Secure counters limit the usage of a certain accessory or consumables to a value preset by the manufacturer. Secure one-way counters can only be decremented.

Delivery form

AuKey chips come in a small form factor SO8N package.

In order to meet environmental requirements, ST offers these devices in different grades of ECOPACK® packages, depending on their level of environmental compliance. ECOPACK® specifications, grade definitions and product status are available at: *www.st.com*. ECOPACK® is an ST trademark.

Tools and services

Leveraging on its wide expertise in secure solutions for banking, government and consumer segments, ST offers a wide range of tools and services to assist the manufacturer.

ST cryptographic experts can advise manufacturers about the definition of optimal security configurations based on the AuKey flexible security and key management architecture. ST can also propose a custom security solution that serves the particular needs of any environment.

AuKey chips are delivered by ST manufacturing plant securely pre-personalized. ST also offers hardware and software tools to support large-scale personalization of AuKey chips at the manufacturer or subcontractor premises. These tools allow to securely generate cryptographic keys and public key certificates, and to load them onto the AuKey chips during the manufacturing process.

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
10-Oct-2009	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