Personal Identity Authentication Module

Datasheet_PIA_Module

P2SD Version7.0.0.5 | July. 19, 2020

PixelAuth Technologies Co., Ltd.

Abstract

Personal Identity Authentication module (PIA),

- Fingerprint/biometric authentication for personal identity
- All fingerprint Enrollment, Matching, authentication is executed on the PIA module.
- Data security managed by secure element in the module.
- Provide multiple interface, easy to integrate into product.
- Provide customization service for special customers’ requests.

The datasheet is intended for those who are considering the integration of the PIA module, into an end product which they are responsible for designing, testing, or manufacturing (“the Design Engineer”). This document seeks to give an in depth look into the information which will assist the Design Engineer in the completion of the task, including, but not limited to the expected performance, the technical characteristics and the electrical characteristics of the module.

*All information subject to change, without further notice.

Revision History

Version	Date	Description
V2.0.0.2	8/12/2016	Update sensor info
V3.0.0.1	7/25/2017	Update product photos
V3.0.0.2	7/28/2017	Correct typos
V3.0.1.1	9/26/2017	New Dimension
V3.0.1.1	11/14/2017	Rename
V3.0.1.5	3/26/2018	New Dimension
V7.0.0.1	2020-01-4	Upgrade to Version 7, remove former revision
V7.0.0.2	2020-2-17	Minor fix
V7.0.0.3	2020-3-15	Add new module
V7.0.0.4	2020-7-17	Add new module
V7.0.0.5	2020-7-19	Add new Features/Services

General notice:

1. All dimension may have tolerance due to different production site.
2. ESD tolerance may be different due to different module design and production.

*All information subject to change, without further notice.

*All information subject to change, without further notice.

Table of Contents

*All information subject to change, without further notice.

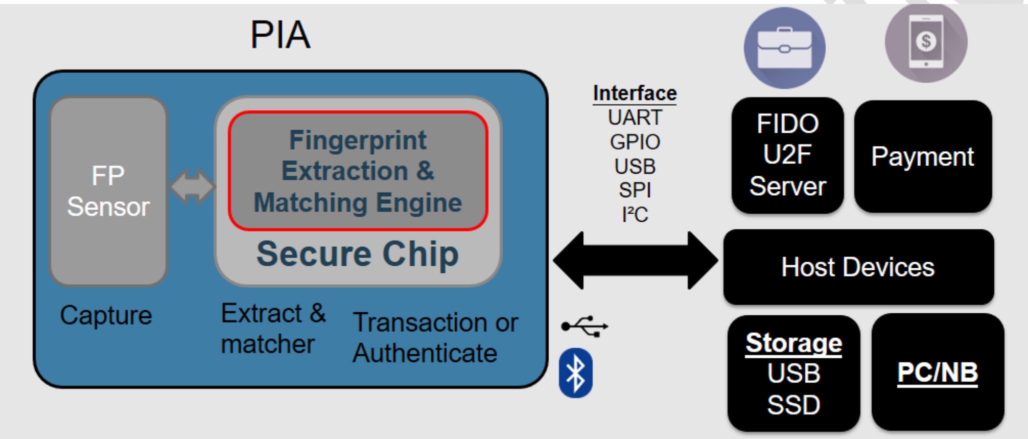
1. Introduction

The **purpose** of the PIA module

is performing the personal identity authentication based on fingerprint.

Key features

- Whole authentication process is executed within the secure chip.
- All fingerprint information is protected and stored within secure chip. To prevent illegal access.
- Rich interface, very easy to connect to host devices.
- Simple API (Application Interface) kit, makes the system integration becomes very easy.



The PIA module includes following main functions:

- Fingerprint touch sensor:
  For abstraction of fingerprint information
- Fingerprint processing unit:
  Perform full function of Fingerprint matching within the PIA, which includes Fingerprint capture, template generating/storage, matching and management.
- Security unit:
  for securing the Fingerprint information/processing and provide security features for authentication.

*All information subject to change, without further notice.

The PIA fingerprint secure module（“the module”）is a small form factor of touch type fingerprint sensor with secure element embedded

For fingerprint sensors, constructed by thousands of highly sensitive capacitive elements with patented sensing architecture, which can capture high resolution images of the fingerprint.

The sensor is powered by a proprietary algorithm which delivers market leading False Acceptance Rate (FAR) and False Rejection Rates (FRR). For these reasons, the Sensor is ideal for integration in many types of consumer electronic devices, including of mobile phones, tablets, notebook PCs, and wearable devices.

Encapsulated and protected by durable molding compound, the Sensor is shielded from impact, scratches, as well as everyday wear and tear. Multiple patented ESD (ElectroStatic Discharge) shielding methodologies are implemented in the sensor level as well as in module level.

With secure element, the fingerprint templates are all stored and processing inside the module to ensure the high level security. Hardware generated crypto keys ensure the high level security on the secure channels between components inside of PIA. Support different kind of security Applications, which includes PKI, PIV authentication and FIDO.

The combination of all of these factors yields state of the art fingerprint authentication module capable of delivering market-leading usability, security, durability and FAR/FRR performance - all rolled up into a tiny module operating at the lowest power consumption in the industry.

*All information subject to change, without further notice.

2. Key Features

Easy to Integrate into Mobile Phones, Tablets, PCs, Wearable Devices and USB Dongles

- Compared to the touch-sensitive fingerprint sensors on the market, it offers maximum design flexibility, smaller size and easier integration
- Modules can be integrated into buttons
- SPI+GPIO

High quality image information

- Dynamic mapping of wet and dry fingers and real-time sensor calibration
- Excellent imaging quality, each sensor pixel with 256 grayscale values
- Effective sensing pixel area size: 103 x 52 pixels

Strict packing protection

- Multi-layer protective packaging can reduce the probability of damage in the process of transportation
- Antistatic packaging, can prevent external electrostatic breakdown module device
- High durability, the module can withstand more than 100,000 touches
- ESD tolerance: +/- 10KV (air discharge), +/- 8KV (contact)
  (Note: This value highly depends on module design and manufacture process)

Low Power Consumption

- Consumption current during normal operation: typical value is 22mA (+/ -10%)
  (Note : Above “Typical value” may be changed due to different cutomized operation mode, ex. faster response time, number of fingerprint compared, security features, etc.)

Environmental regulation

*All information subject to change, without further notice.

- Pass the lead-free certification
- Green certification
- Operating temperature :-20℃~ + 60℃
- Humidity :0% ~ 90% RH at 60℃

High quality algorithm

- FAR<1/50000 FRR < 3%
- Best identify approving time: 300ms

  Approving time may be longer due to the increasing of fingerprint template number

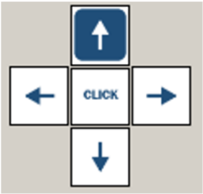
*All information subject to change, without further notice.

New Features Customization service (NRE Based service)

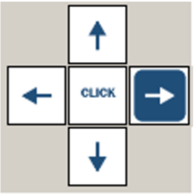
- Based on customer’ s needs/requirements to do system modification.

- **Swap enroll** supported
  A simple and effective way to collect fingerprint, Only 1-3 swipes for enrollment process.

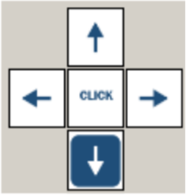
- **Navigation** supported :
  Provide push bottom-like function, replace physical bottoms



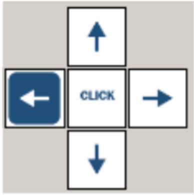
Up



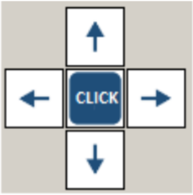
Right



Down



Left



Click

- Block chain application: Perform Cold wallet features.
- Other security features .....

*All information subject to change, without further notice.

3. Architecture

As shown in Fig. 1, PIA communicates with external host through spi. Spi SSN serves as chip selection pin, CLK serves as clock pin, and GPIO serves as interrupt pin for receiving data.Strict communication protocol guarantees the security and efficiency of communication between module and host.It makes designing products more flexible.

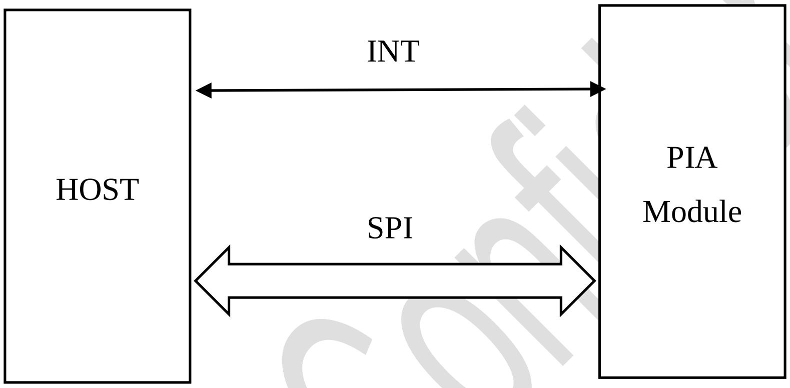


Fig.1 Basic system block diagram

The flexible PIA authentication protocol is defined for the host sending command and host acquiring command.

*All information subject to change, without further notice.

4. Physical Module Information

TYPE	Maximum number of fingerprints can be stored
P2SDS-NABL2-S05	Up to eight fingerprint templates can be stored (Please contact with InCOMM for the detail)

P2SDS-NABL2-S05 Size diagram is as follows:

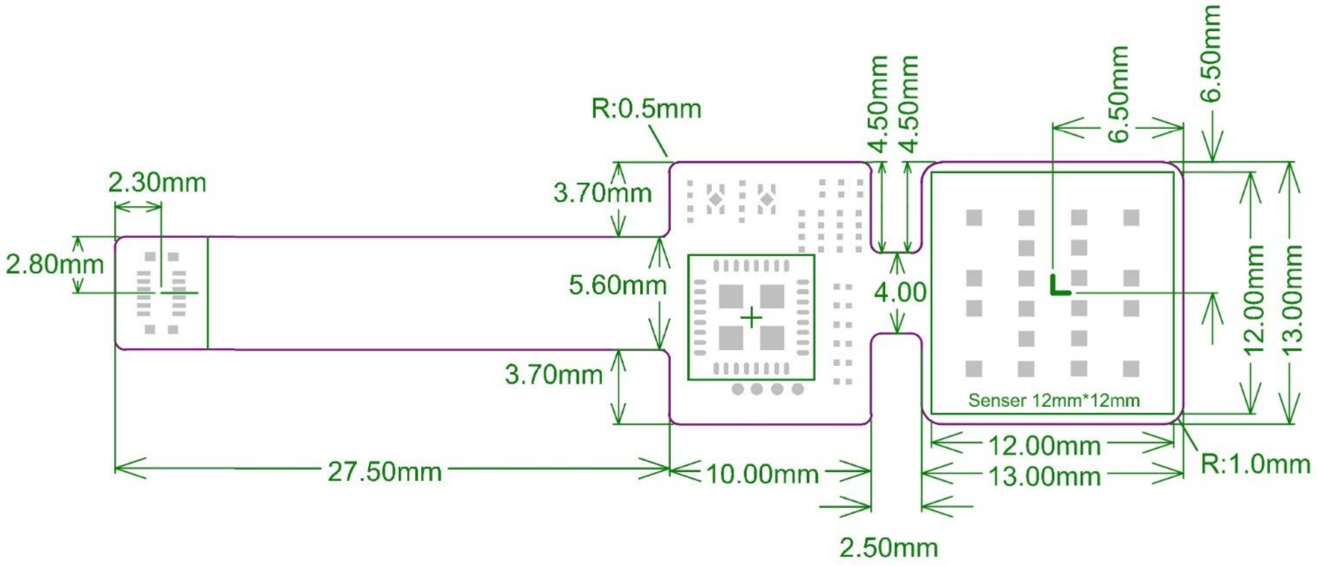


Fig. 2 Size Chart-Bottom View

*All information subject to change, without further notice.

P2SDS-NABL2-S05 Pin function definition and pin distribution diagram are as follows

1	VCC
2	VCC
3	GND
4	GND
5	SPI_MISO
6	SPI_MOSI
7	UART_TX
8	SPI_CLK
9	UART_RX
10	SPI_SSN
11	INT
12	GPIO

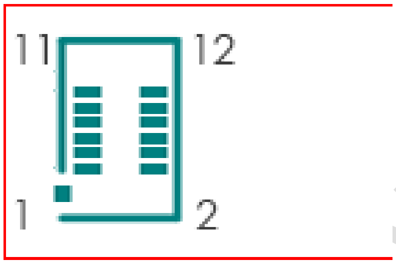


Fig. 3 Pin Sequence- Bottom View

5. Pin description

Pin	Min	Typ	Max	Direction	Parameter
VCC	4.5V	5V	5.5V	VCC	VCC voltage level
GND				VDD	VDD voltage level
SPI MISO		1.8V		IN/OUT	SPI MISO
SPI MOSI		1.8V		IN/OUT	SPI MOSI
SPI CLK		1.8V		IN/OUT	SPI CLK
SPI SSN		1.8V		IN/OUT	SPI CS
INT		1.8V		OUT	Interrupt the pin, which generates a level change when fingerprint module has data to send
UART TX		1.8V		OUT	UART TX
UART RX		1.8V		IN	UART RX
GPIO		1.8V			reserved

Table 1 Pin Description

*All information subject to change, without further notice.

6. Electrical characteristics

Symbol	Parameter	Condition	Min	Typ	Max	Unit
VCC	VCC voltage level	5	4.5	5	5.5	V
I_{RUN}	Module normal operating current	22mA@5V	22mA@5V			
I_{ENR}	Peak current when fingerprint input for module	28mA@5V	28mA@5V			
TAMB	Operating temperature		-20	25	85	°C

Table 2 module power supply characteristics

*All information subject to change, without further notice.

7. Customized Services

Provide customization service to meet customer’ s special requirements.

- Need do assessment to make sure the requirement is feasible.
- NRE may be incurred.

7.1 General

- Navigation: Up/Done/Right/Left, Long Click/Double Click
- Swipe Enroll

7.2 Security

Cryptocurrency wallet: (HDKD)

- Modules uses a financial-level secure element to enable seed generation and storage, ensuring the secure management of users’ digital assets
- Modules integrates fingerprint identification technology, which ensures the security and enables it more convenient
- BTC、ETH(including ERC20)、EOS、USDT、XRP、LTC、ETC、NEO Supported

Algorithm support

- Message Digest: RIPEMD160, SHA224, SHA256, SHA384, SHA512, SHA3, KECCAK, BLAKE2B
- DES (56, 112, 168 bits), AES (128, 192, 256 bits),
- ECC (256 bits), RSA (1024, 2048bits), HMAC Signature: HMAC-SHA256,
  Elliptic Curve Signature SECP256K1, SECP256R1

*All information subject to change, without further notice.