FPC AllKey Pro – Supplementary Information

Additional features

- Secure communication
- Enhanced biometric spoof detection
- Navigation Pointing Stick mode
- Support for 45 enrolled fingers
- Configurable enrollment
- Template import/export
- I2C protocol interface
- USB protocol interface

General description

Fingerprints Biometric System device family FPC2530 offers a proven, robust fingerprint sensor solution that can easily be integrated into virtually any application. Fingerprint templates are automatically created and stored in the internal flash memory. The device can be controlled from any host with basic commands for enrollment and verification or be customized for stand-alone operation without external components. Fingerprints Biometric System device is provided with several different host interfaces, pre-loaded software and is ready to use on delivery. The Biometric System device comes with an appealing black coating, that together with a built-in hidden discharge node (bezel) provides protection against ESD, scratches, impact, and everyday wear and tear.

The Pro version described in this document offers an extended feature set that supports two additional communication interfaces and encrypted communication for applications where security is a high priority. It also allows the transfer of enrolled fingers between devices, to open for multiple AllKey-devices working together.

Table of Contents

1 INTRODUCTION

1.1 Document content

This specification outlines the extended feature set which comes with the FPC AllKey Pro Biometric System. It acts as a complement to the general Product Specification; everything included there, such as mechanical and environmental information, integration guidelines and packing, is still applicable. This document only highlights what is specific to FPC2534AP and FPC2534AM.

1.2 FPC2530 device family

The FPC AllKey Biometric System device family includes several biometric system devices, with different interface configurations and system functionalities. Most versions are available with a hardware compatible electrical and mechanical interface, allowing for future upgrades without the need for redesign.

Versions within the FPC2530 AllKey family at present date:

PRODUCT	DESCRIPTION	PRODUCT SPECIFICATION	FEATURE SUPPLEMENT
FPC2532AP	AllKey Biometric System LGA	FPC2530	
FPC2532AM	AllKey Biometric System Module	FPC2530	
FPC2534AP	AllKey Pro Biometric System LGA	FPC2530	FPC2534 (this document)
FPC2534AM	AllKey Pro Biometric System Module	FPC2530	FPC2534 (this document)

1.2.1 FPC2532 AllKey

FPC2532 standard version is fully covered in the generic Product Specification. This product target applications where fingerprint is used to increase convenience by adding Identification, Personalization and Navigation. The FPC2532 is available both in an LGA package FPC2532AP, and a versatile flex module assembly FPC2532AM.

1.2.2 FPC2534 AllKey Pro

FPC2534 high security version is covered in this Feature Supplement. This products target applications where fingerprint is used for Authentication and where Protection for Tampering is priority. The FPC2534 is available both in an LGA package FPC2534AP, and a versatile flex module assembly FPC2534AM.

2 SECURITY

FPC AllKey Pro supports encrypted host communication. The cipher for encryption and decryption is AES with GCM and GMAC authentication. Both 128- and 256-bit AES keys are supported.

When FPC AllKey Pro is shipped it comes without secure communication enabled. All functions are available in non-secure mode only.

To enable secure mode, the host sends an AES key to the FPC AllKey Pro module. This is made once and cannot be undone without doing a special factory reset operation. The key is shared between the host and FPC AllKey Pro and is used for all future communication. The host is responsible for generating the key and it's recommended to use a true random generator or similar for it. The key should be securely stored on host.

2.1 Encrypted communication

The commands are structured the same way for secure and non-secure mode. The supported commands in the different modes are however different.

2.1.1 Operation

A random 12-byte IV (initialization vector) is created, and included, in each transfer. In addition, a 16-byte GMAC tag is also included in the transfer. Including these additional fields modifies the host protocol as described below.

Non-Secure Transfer

Frame Header	Command (Frame header payload) Plain Text
Payload size = x	Size = x

Secure Transfer

Frame Header	IV	GMAC Tag	Command (Frame header payload) ENCRYPTED
Payload size = x + 12 + 16	Size = 12	Size =16	Size = x

The additional fields for IV and GMAC tag are placed right after the frame header. This affects the frame header *payload_size* parameter, which is increased by 12 + 16 = 28 bytes.
The Frame Header *flags* parameter has the FPC_FRAME_FLAG_SECURE bit set to identify that it is a secure and encrypted transfer.

The Frame Header, IV and GMAC Tag are transferred in plain text. The Command data is encrypted. Since GCM is counter mode based, the plain text and cipher text are the same size, and no padding is needed.

2.1.2 GMAC

The Authentication tag calculation includes the Frame Header as AAD (Additional Authentication Data) and the Command Data.

2.2 Key Provisioning

The key size is set in the key provisioning. The key is set via the Set Crypto Key command.
Once the key is set, all biometric commands must be encrypted. They can no longer be run un-encrypted.

3 INTERFACES

3.1 USB communication

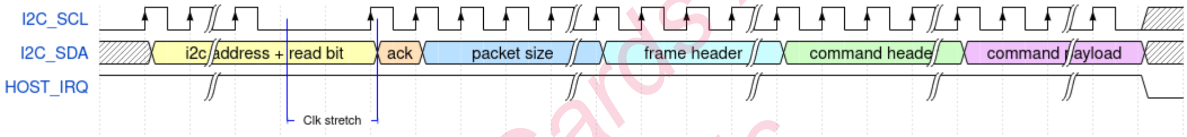
FPC Allkey Pro supports the host protocol over USB using the USB CDC ACM protocol. See UART communication for further details on how to use the host protocol over USB.

3.2 I2C communication

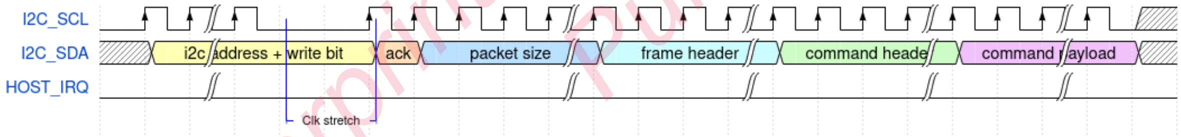
In I2C mode, there are some additions compared to the normal protocol headers. The I2C address + rw bit is sent first, after that 2 bytes of I2C packet size are sent before the normal frame header, command header etc. are sent.

The host must support clock stretching since the FPC Allkey Pro module will utilize that during transfers. This is needed both for wakeup from deep sleep and during normal transfers. Default address is 0x24 (7 bit) and is configurable, see Section 4.4. The HOST_IRQ line will go high when the device has something to send.

I2C Device to Host



Host to Device



4 SOFTWARE

4.1 States

The internal states of the software are similar between the Standard and Pro variants; they are represented by a 2-byte bitmap, where some states are mutually exclusive. For example, only one of Enroll, Identify, Navigation, and Capture can be active at a time. Attempting to enter multiple of these states simultaneously yields an error response. The state highlighted in **bold** is exclusive to FPC AllKey Pro.

STATE ID	NAME	CLEARED ON ABORT	DESCRIPTION
0x0001	App FW Ready	No	Application is ready to receive commands.
0x0002	**Secure Interface**	**No**	**Secure mode is enabled - most commands must be sent encrypted. Refer to Commands section to see which commands are affected.**
0x0004	Capture	Yes	Sensor is armed for a single touch. Transitions to *Image Available* state on capture. Note that the image cannot be used for biometric operations; this state is intended for debugging purposes and evaluating image quality.
0x0010	Image Available	Yes	A captured fingerprint image is available for readout. No biometrics can be performed on the image. State is cleared upon readout.
0x0040	Data Transfer	Yes	Data transfer session is ongoing.
0x0080	Finger Down	No	A finger is touching the sensor. Can only be entered if the sensor is actively searching for a finger (i.e. during Enroll, Identify, Navigation, or Capture).
0x0400	System Error	No	A system error has occurred. State will clear itself once the error status has been read out.
0x1000	Enroll	Yes	Enrollment of a new user is ongoing, and the sensor is armed for multiple touches. State will clear itself once enrollment finishes.
0x2000	Identify	Yes	Identification/Verification of user is ongoing, and the sensor is armed for a single touch. State will clear itself once the match result is reported.
0x4000	Navigation	Yes	Sensor is armed for detection of navigational gestures.

4.2 Commands

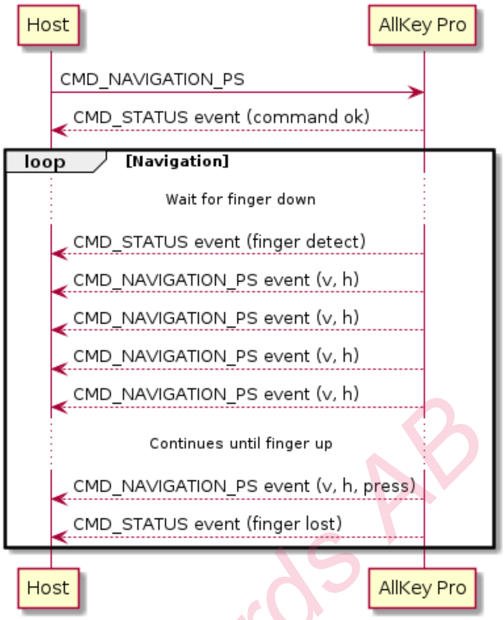
The table below shows a summary of all commands supported in AllKey Pro. Commands which are exclusive to the Pro variant are written in **bold**, and the 'S' column indicates commands that will only work in secure mode when security is enabled.

ID	NAME	S	DESCRIPTION
0x0040	Status		Get the status of device.
0x0041	Version		Get FW version.
0x0044	Built-in Self-Test (BIST)		Run internal test for defects on the fingerprint sensor.
0x0050	Capture	X	Arm the sensor to capture a single image on touch.
0x0052	Abort	X	Abort active state(s). See Section **Error! Reference source not found.** for which states can be aborted.
0x0053	Image Data	X	Request readout of fingerprint image collected in *Capture* mode.
0x0054	Enroll	X	Put the device in Enrollment state. The device will register each touch of the sensor until enrollment finishes.
0x0055	Identify	X	Put device in Identify state (one touch) to perform matching against saved templates.
0x0060	List Templates	X	List enrolled templates.
0x0061	Delete Template(s)	X	Delete one or all enrolled templates.
0x0062	**Template Get**	**X**	**Request readout (export) copy of a template from the device to host.**
0x0063	**Template Put**	**X**	**Request sending (import) of a template from host to the device.**
0x006A	Get System Configuration		Get active or default system configuration settings.
0x006B	Set System Configuration	X	Set system configuration settings.
0x0072	Reset		Reset device.
0x0083	**Set Crypto Key**	**X**	**Perform key provisioning for encrypted communication. The device must be reset afterwards for it to take effect. See Section 2.2 for details.**
0x00B0	Set Debug Log Level	X	Not supported. Only error logs can be read out.
0x00FA	**Factory Reset**		**Wipe all templates and encryption key from the device. This command is only allowed if the appropriate system configuration flag is set (disabled by default).**
0x0101	Data Get	X	Read out one chunk of requested data from buffer. A data get request, such as *Image Data*, must be sent prior.
0x0102	**Data Put**	**X**	**Write one chunk of requested data from host. A data put request, such as *Template Put*, must be sent prior.**
0x0200	Navigation - Gesture	X	Put the device in gesture-based Navigation mode.
0x0201	**Navigation - Pointing Stick**	**X**	**Put the device in pointing-stick based Navigation mode.**
0x0300	GPIO Control	x	Set or get configuration for GPIO pins.

4.3 Pointing stick navigation

The FPC2534 comes with an additional mode of navigation: *pointing stick*. Instead of detecting a set of gestures, the device will continuously send information about every 10 ms of the finger position on the sensor using a horizonal and vertical value (+-36). This allows it to function like a pointing stick commonly found on laptop keyboards for controlling the cursor. The events also include a gesture value that will indicate if a press is detected when the finger is lifted (only when no movement has been detected for some time prior to finger lift).

Navigation events are sent to the host as seen in the diagram below. To exit navigation, an abort request must be sent from the host.


Host
AllKey Pro
CMD_NAVIGATION_PS
CMD_STATUS event (command ok)
loop
[Navigation]
Wait for finger down
CMD_STATUS event (finger detect)
CMD_NAVIGATION_PS event (v, h)
CMD_NAVIGATION_PS event (v, h)
CMD_NAVIGATION_PS event (v, h)
CMD_NAVIGATION_PS event (v, h)
Continues until finger up
CMD_NAVIGATION_PS event (v, h, press)
CMD_STATUS event (finger lost)
Host
AllKey Pro

4.4 System configuration

A few parameters for the software can be configured by the host. The table below lists all available settings and their default values. Rows written in **bold** are only available in the Pro version. These are FPC recommended settings, and do not need to be changed.

CONFIG		DEFAULT	DESCRIPTION
Version		2	Version of system configuration structure. Not to be changed.
Finger Scan interval		34 ms	Sleep time between each finger presence check. A higher value will decrease power consumption in Finger Detect Mode, but also increase response time.
System Flags	Status event at boot	Enabled	Send Status event after system boot.
	Stop mode for UART	Disabled	Let system go into deep sleep when using UART interface. This requires the system to be woken via the wake-up pin (CS) before sending any UART data to host.
	UART IRQ before TX	Enabled	Set IRQ pin before SiP sends UART data. The delay between the IRQ and start of data transfer is configurable via “UART delay before TX” below.
	Allow Factory Reset	**Disabled**	**Allow the *factory reset* command, which wipes encryption key, enrolled fingers, and system settings. It is recommended to only enable this flag for development purposes.**
UART delay before TX		1 ms	Delay between the IRQ pin is set, and UART TX is started.
Idle time before sleep		0 ms	Idle time after last command before entering deep sleep.
Identify lockout	Max consecutive fails	5	Number of consecutive fails to trigger a lockout. The lockout is activated on the next failure i.e. 6th no-match for default setting.
	Lockout time	15 s	Lockout time. The lockout is cleared upon FW reset.
Enrollment	**Total no. touches**	**12**	**Required number of accepted touches for enrolling a new finger.**
	Immobile touches	**0**	**Max number of immobile touches taken into an account. See section 4.5 for details.**
I2C address		**0x24**	**7bit I2C Address**

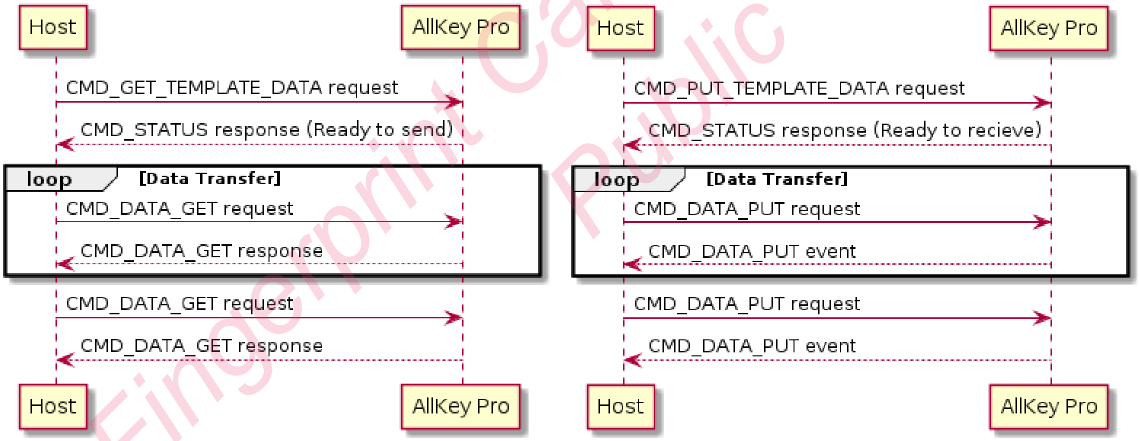
4.5 Enrollment configuration

The number of touches required during enrollment can be changed through the System Configuration. It includes two parameters – number of touches, and number of *immobile* touches. The former specifies the maximum number of accepted touches are required during enrollment and the latter reduces the minimum number of accepted touches. For example, a configuration with 12 total touches and 4 immobile will require 8-12 touches for enrollment. Moving the finger around from touch to touch helps registering a larger part of the fingerprint and thus requires fewer total touches for similar performance.

It is worth noting that strong successful verifications will update the registered template with the new information, referred to Template Update (TU). This will compensate for a shorter enrollment but at the cost of a longer "learning period" – eventually the performance will be independent of the enrollment setup.

4.6 Template import/export

FPC Allkey Pro supports sending fingerprint templates to and from the device, which can be used for e.g. storing them externally or synchronizing templates across multiple devices. The size of a template is 18kB and needs to be sent/read in multiple chunks. The transfer is initialized by a *Template Get* or *Template Put* command from the host, followed by repeated *Data Get*/*Data Put* requests until the entire template is transferred. An overview of the procedure is also seen in the diagram below.



5 PERFORMANCE

5.1 Timings

Below are timing and performance values for FPC AllKey Pro. Note that a response is always sent from the device once an operation finishes, such as *identify*. Measurements are independent of the communication interface used.

USE CASE	VALUE	COMMENT
Power up / Boot	170 ms	Status is sent from device to host when finished. This can be disabled in System Configuration. Timing is identical for a SW reset.
Wakeup from deep sleep	500 us	The device typically wakes up faster; this is the lowest recommended delay between sending a wakeup signal and data.
Enrollment	130 ms	-
Identify	160 - 2050 ms	Depends based on number of fingers enrolled and the match ID; it goes through all registered ID:s in ascending order and stops on the first match. Specifying an ID in the verify request will always yield the best-case scenario.

5.2 Biometric performance

The Pro version includes enhanced matching algorithm with extra security to better detect spoofs i.e. faked fingerprints. Such detection always comes with a slightly increased False Reject Rate (FRR). The increase in FRR is primarily seen for drastically varying skin conditions; under normal conditions the difference is unnoticeable.

PARAMETER	USE CASE	VALUE	COMMENT
FRR (False Reject Rate)	After Enrollment	< 5.0 %	Normal dataset, measured directly after enrollment
	After Template Update	< 1.5 %	Normal dataset, measured after multiple updates
	Wet Fingers	< 10 %	Dataset with wet fingers, measured against normally enrolled fingers
FAR (False Accept Rate)	-	1 / 100 K	False Accept Rate is given per finger

5.3 Power consumption

Power consumption is identical between the *Standard* and *Pro* versions of FPC AllKey. It is also similar across all communication interfaces except for USB, which is higher. For a full list of electrical characteristics, refer to the FPC2530 Product Specification

PARAMETER	CONDITION	VALUE	
		SPI, UART, I2C	USB
Finger detect mode (FDM)	Waiting for finger	22 uA	211 uA
Active mode	Processing commands	5.2 mA	5.4 mA
Deep sleep mode	-	14 uA	204 uA

6 REVISION HISTORY

REVISION	DESCRIPTION	RELEASE DATE
PA1	Final release (CS)	Dec 2024

7 CONTACT INFORMATION

Fingerprint Cards AB

Main office
P.O. Box 2412
SE-403 16, Gothenburg
Sweden

Web site
www.fingerprints.com

Sales contact information: sales@fingerprints.com