

**TRUSTCRYPT
WHITE PAPER
ISSUE A**

The information contained herein is the property of ST Electronics (Info-Security) Pte Ltd and may not be copied, used or disclosed in whole or in part to any third party except with written approval of ST Electronics (Info-Security) Pte Ltd or, if it has been authorized under a contract.

TRUSTCRYPT WHITE PAPER

Contents

TITLE/AUTHORIZATION	i
CONTENTS	I
LIST OF ILLUSTRATIONS	II
LIST OF ABBREVIATIONS	III
1. INTRODUCTION	1
2. TRUSTCRYPT OVERVIEW	1
3. TRUSTCRYPT APPLICATIONS	2
3.1 AS A STAND-ALONE DEVICE USING DEFAULT FIPS-CERTIFIED APPLICATION.....	2
3.1.1 <i>Guidelines to Use Default FIPS-certified Application</i>	3
3.2 AS AN INTEGRATED MODULE RUNNING CUSTOMIZED APPLICATION IN NON-FIPS MODE.....	4
4. SPECIFICATIONS	6

List of Illustrations

FIGURE 1 TRUSTCRYPT	1
FIGURE 2 TRUSTCRYPT DEFAULT APPLICATION SETUP	2
FIGURE 3 EXAMPLE OF TRUSTCRYPT CUSTOMIZE APPLICATION SETUP.....	5

List of Abbreviations

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher-Block Chaining
CFB	Cipher Feedback
CPU	Central Processing Unit
DRNG	Deterministic Random Number Generator
ECB	Electronic Codebook
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FPGA	Field-Programmable Gate Array
GPIO	General Purpose Input Output
Hz	Hertz
KB	Kilobytes
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
mA	Milliamperere
mm	Millimeters
NIST	National Institute of Standards & Technology
OFB	Output Feedback
PKCS	Public-Key Cryptography Standards
RFI	Radio Frequency Interference
RS232	Recommended Standard 232
RSA	Rivest, Shamir and Adleman
RX	Receive
SHA	Secure Hash Algorithm
SRAM	Static Random Access Memory
TX	Transmit
UART	Universal Asynchronous Receiver/Transmitter
USA	United States of America
V	Volts

THIS PAGE IS LEFT BLANK INTENTIONALY

1. Introduction

Security is important in protecting sensitive information. TrustCrypt provides a secure platform that is certified by National Institute of Standards & Technology (NIST). With this certification, it gives user the assurance that TrustCrypt has a high level of security as it is designed and implemented according to the strict requirement by Federal Information Processing Standard (FIPS).

2. TrustCrypt Overview

The DigiSAFE TrustCrypt is a multi-chip embedded module that is FIPS 140-2 level 3 security level certified (Certificate Number 1304). Federal Information Processing Standard (FIPS) is governed by the National Institute of Standards & Technology (NIST)/USA and CSA/Canada. It is a standard for the protection of valuable and sensitive information

DigiSAFE TrustCrypt is a programmable cryptographic module designed to support high assurance applications and provide secure cryptographic resources, including secure key generation and storage. It is built upon a secure physical enclosure and contains a secure bootstrap which authenticates application loading.

The security services provided by TrustCrypt are AES, SHA, RSA and DRNG through the RS232 serial port.

Customized application can be downloaded into the TrustCrypt if needed. The customized application to be downloaded must be signed by an approved authority using RSA.

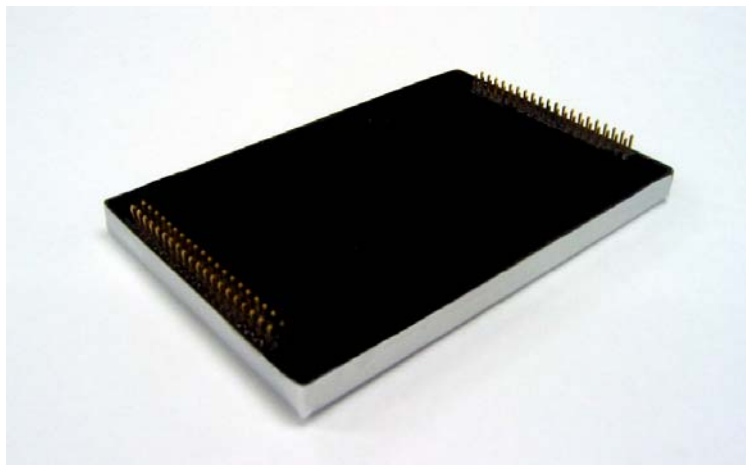


Figure 1 TrustCrypt

3. TrustCrypt Applications

TrustCrypt is generally employed in one of the following configuration:

- As a stand-alone device running the Default FIPS-certified Application
- As an integrated module running Customized Application in non-FIPS mode

3.1 As a Stand-Alone Device Using Default FIPS-certified Application

In this mode, TrustCrypt is operated as Cryptographic co-processor to offer the default cryptographic services.

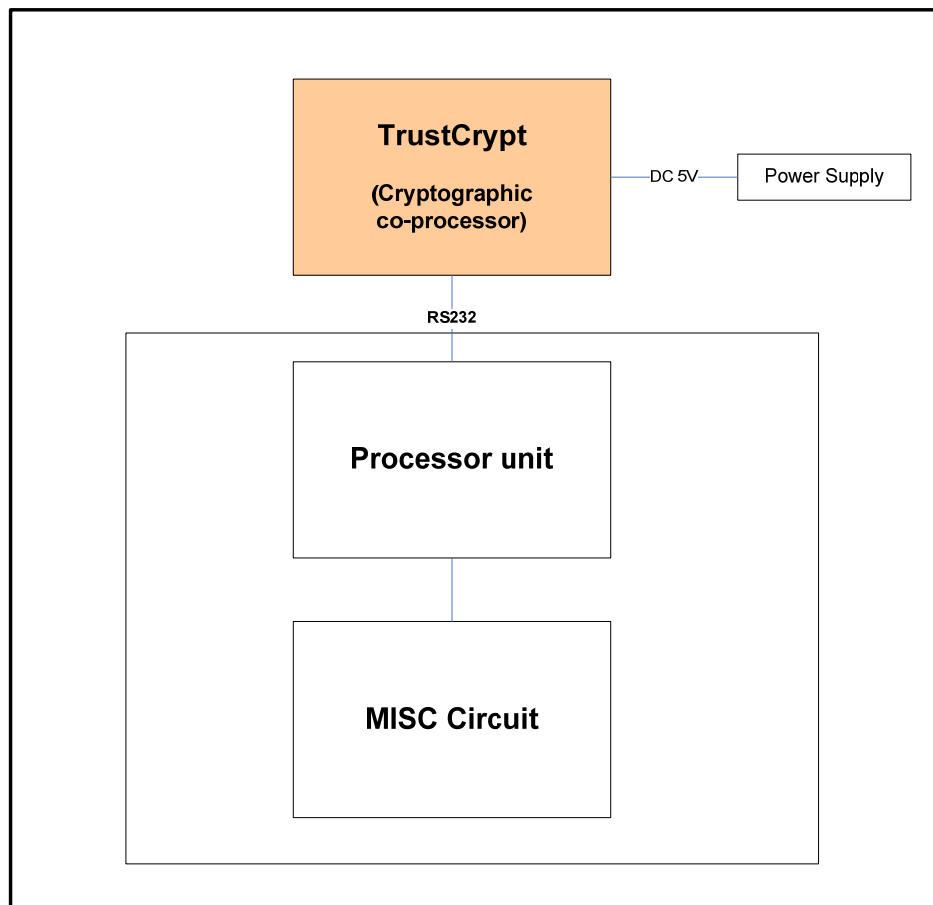


Figure 2 TrustCrypt Default Application Setup

TrustCrypt will undergo boot, self-tests, and thereafter run the Default Application in User Mode when +5V is applied to the power pins. The following list of services will be made available via the RS232 pins :

- AES 128, 192, 256 in ECB, CBC, OFB, CFB128 mode.
- SHA-256 and SHA-512
- RSA 1024 and 2048 using PKCS v1.5
- DRNG with AES-128 (ANSI X9.31)

Please refer to the TrustCrypt Security Policy (G-P6021-TM003) for the details of the services provided.

3.1.1 Guidelines to Use Default FIPS-certified Application.

Once the TrustCrypt is in the default application User Mode, the default services are available. In order to call the available services, the information must be sent through the RS232 serial port. The data must be packed into the specified defined packet format (with header, data and frame check sequence) before it is sent to the TrustCrypt. After TrustCrypt processed the request, it will reply through the RS232 serial port with a specified format.

The specified format of the packet will be provided by ST Electronics (Info-Security).

3.2 As an Integrated Module running Customized Application in non-FIPS mode

The customized application must be coded, compiled and packaged following the guidelines given by ST Electronics (Info-Security). The customized application package will be signed by the publishing authority before it is downloaded into TrustCrypt through the serial port.

If a Customized Application has been loaded and +5V is applied to the power pins, TrustCrypt will boot, execute the self-tests and thereafter run the Customized Application instead of the Default Application.

The Customized Application has the option of making use of more of TrustCrypt's pins and functions as these are made available to the Customized Application once TrustCrypt is running in this configuration.

The list of additional pins and functions available to the customized application includes and is not limited to the following:

- 2 additional UART and their corresponding TX and RX pins for a total of 3 customizable UARTs
- Use of NIST compliant on-board Hardware True Random Number Generator
- Use of 128KB battery backed-up, tamper protected SRAM for storage of sensitive data
- Battery supply input pin for a +3V Battery source to maintain the SRAM when main power is turned off
- Anti-Tamper cum Emergency Erase input pin to trigger the Trustcrypt CPU and concurrently erase the SRAM during both main power on and power off states.
- Vstandby output pin that provides 3.3V when main power is present and automatically switches to source from the 3V battery when main power is absent, thereby maintaining an always on 3.0-3.3V power supply (up to 30mA). This signal is used as a source for external tamper sensor.

- Up to 30 customizable GPIO pins
- 16-bit multiplexed Databus for fast data transfer to external FPGA or to peripheral devices like LCD, keypad etc.
- Software libraries for the list of Default Application cryptographic services
- Any other functions which are run by the Customized Application

The following diagram illustrates how TrustCrypt might be employed in this configuration. The TrustCrypt databus is used to interface with an FPGA that performs high speed encryption / decryption for example, or to another co-processor or main processor.

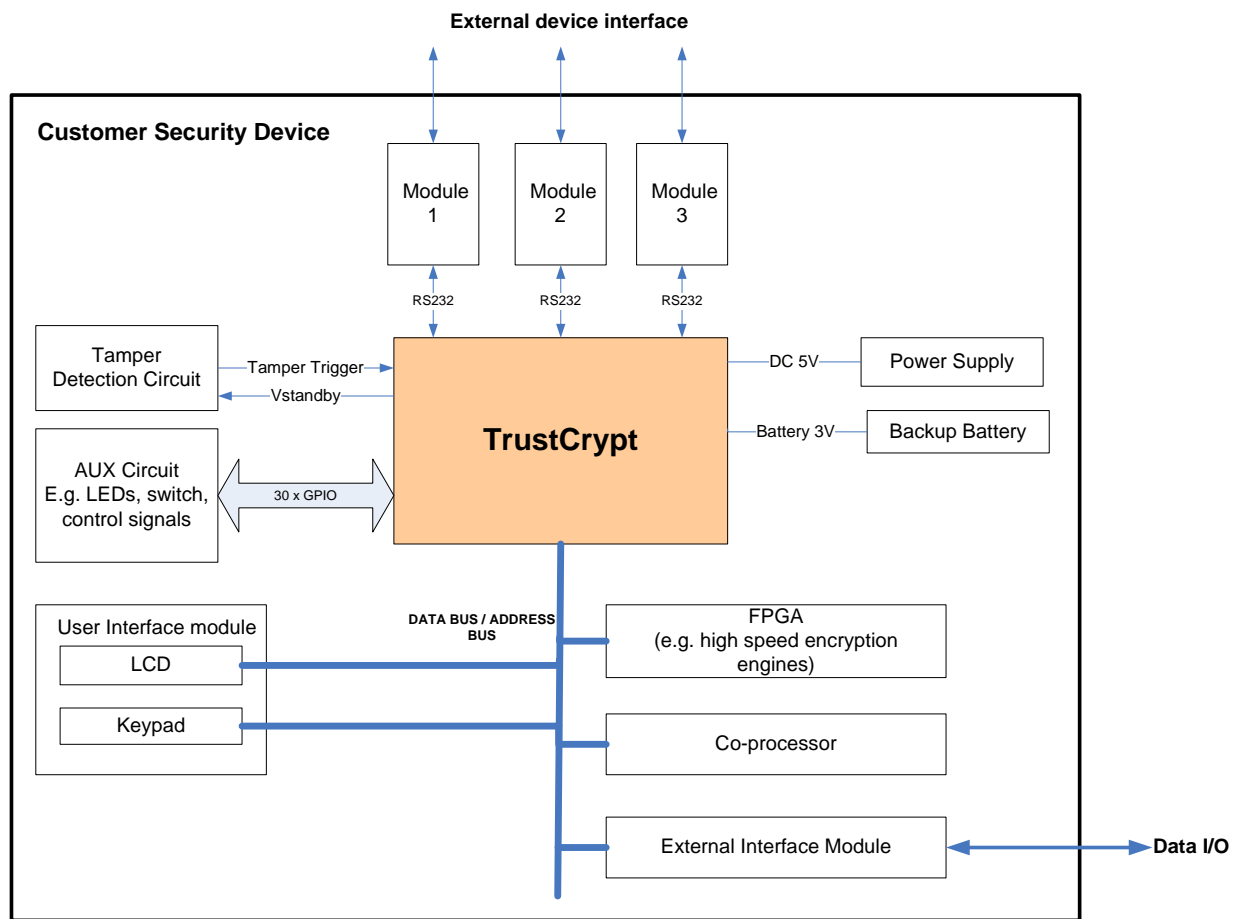


Figure 3 Example of TrustCrypt Customized Application Setup

4. Specifications

General

- FIPS 140-2 level 3 certified (certificate number 1304)
- Battery Backup of cryptographic variables

Cryptography / Authentication

- AES 128, 192, 256 in ECB, CBC, OFB, CFB128 mode.
- SHA-256 and SHA-512
- RSA 1024 and 2048 using PKCS v1.5
- DRNG with AES-128 (ANSI X9.31)

Security

- Encased in a hard opaque commercial grade epoxy.
- Active zeroization of cryptographic data.
- KEK Publishing Authority for downloading Key
- Application Publishing Authority for downloading customized application.

Diagnostics

- Automatic Power-up self-tests

Interface

- RS232 UART
- GPIO pins

Operating Environment

- Operating temperature: 0°C to +50°C
- Relative Humidity: 0 to 90%
- Meets FCC Part 15, Class B EMI/RFI requirements

Electrical & Mechanical

- Mains: 5VDC
- Dimension: 85W x 10H x 55Dmm

ST Electronics (Info-Security) Pte Ltd

100 Jurong East Street 21, ST Electronics Jurong East Building,
Singapore 609602
Tel: (65) 6568 7118 Fax: (65) 6568 7226
Email: info@digisafe.com URL: www.digisafe.com
(Regn. No.: 199902746G)

