DIGISAFE®
CONNECTING SECURELY

# TrustCrypt

## Security Policy

ST Electronics
(Info-Security)

ST Electronics
A company of ST Engineering

# TRUSTCRYPT

# SECURITY POLICY

## G-P6021-TM003
## (ISSUE A)



ST Electronics (Info-Security) Pte Ltd
ST Electronics Jurong East Building
100 Jurong East Street 21
Singapore 609602
Tel: (65) 6568 7118 Fax: (65) 6568 7226
Email: info@digisafe.com
URL: www.digisafe.com

# DIGISAFE TRUSTCRYPT SECURITY POLICY

# Contents

# 1. Module Overview

The ST Electronics DigiSAFE TrustCrypt Module version 1.0.0 (the "module") is a FIPS multi-chip embedded cryptographic module encased within a secure hard opaque commercial grade epoxy. The primary purpose for this module is to provide cryptographic services to users including ciphers such as AES 256, RSA 1024, RSA 2048, SHA-256, and SHA-512. Additionally the module contains a secure bootstrap which authenticates both customized application loading & bootloading.

The module is comprised of the following HW/FW components:

- Module HW P/N 9910-8000-0624
- Glue Code executed in the module's CPLD – FW version 1.0.0
- Crypto Libraries executed in the module's Marvell XSCALE PXA300 processor – FW version 1.0.0
- Kernel Operating System executed in the module's Marvell XSCALE PXA300 processor – FW ARM-Linux 2.6.21
- Bootstrap Application executed in the module's Marvell XSCALE PXA300 processor – FW version 1.0.0

# 2. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

**Table 1 - Module Security Level Specification**

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module Specification | 3 |
| Module Ports and Interfaces | 3 |
| Roles, Services and Authentication | 3 |
| Finite State Model | 3 |
| Physical Security | 3 |
| Operational Environment | N/A |
| Cryptographic Key Management | 3 |
| EMI/EMC | 3 |
| Self-Tests | 3 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |

# 3. Modes of Operation

## *3.1 Approved Mode of Operation*

The DigiSAFE TrustCrypt Module only supports an Approved mode of operation - FIPS mode. The module supports Approved mode of operation indicators. Upon power up the module sends a system information packet containing the module version number, release date, and other module information out its console port. Additionally after the module performs its FIPS power-on self-tests it sends a self-test state packet to the console port containing 1 byte for pass/fail of each power-on self-test. Please see the module's operator guidance documentation for the technical details on how to obtain the module's Approved mode of operation indicators.

It is important to note that only the above mentioned Glue Code, Crypto Libraries, Kernel Operating System, and Bootstrap Application FW were tested and validated to FIPS 140-2. Once the module loads a customized application (Load Customized Application service allocated to the module's Crypto-Officer role) the module transitions into a state that is outside the scope of this validation. Also note that customized applications must always be signed by an ST Electronics Application Publishing Authority and the module verifies the signature when performing its Load Customized Application service. Writers of Customized Applications must undergo a separate FIPS 140-2 validation if they want the combined entity [DigiSAFE TrustCrypt + Customized Application] to be certified as a FIPS module.

The cryptographic module implements FIPS Approved algorithms as follows:

1. AES-128 ECB Mode Encrypt/Decrypt (Cert. #932)
2. AES-128 CBC Mode Encrypt/Decrypt (Cert. #932)
3. AES-128 CFB Mode Encrypt/Decrypt (Cert. #932)
4. AES-128 OFB Mode Encrypt/Decrypt (Cert. #932)
5. AES-192 ECB Mode Encrypt/Decrypt (Cert. #932)
6. AES-192 CBC Mode Encrypt/Decrypt (Cert. #932)
7. AES-192 CFB Mode Encrypt/Decrypt (Cert. #932)
8. AES-192 OFB Mode Encrypt/Decrypt (Cert. #932)
9. AES-256 ECB Mode Encrypt/Decrypt (Cert. #932)
10. AES-256 CBC Mode Encrypt/Decrypt (Cert. #932)
11. AES-256 CFB Mode Encrypt/Decrypt (Cert. #932)
12. AES-256 OFB Mode Encrypt/Decrypt (Cert. #932)
13. SHA-256 Hashing (Cert. #915)
14. SHA-512 Hashing (Cert. #915)
15. RSA-1024 PKCS1.5 Signature Verification and Generation (Cert. #451)
16. RSA-2048 PKCS1.5 Signature Verification and Generation (Cert. #451)
17. DRNG ANSI X9.31 Appendix 2.4 (output of random numbers– no key generation) (Cert. #533)

The cryptographic module implements FIPS allowed algorithms as follows:

1. AES Key Wrapping performed in compliance with the AES Key Wrap Specification (Draft), published by the National Institute of Standards and Technology on 16 November 2001. This is an allowed key transport mechanism as per FIPS 140-2 Implementation Guidance 7.1. (AES Cert. #932, key wrapping; key establishment methodology provides 256 bits of encryption strength)

2. Hardware NDRNG (FIPS 140-2 Annex C: "There are no FIPS Approved nondeterministic random number generators"). The module implements the NDRNG for outputting random numbers and seeding the DRNG.

# 4. Physical Security

## *4.1 Dimensions*

The DigiSAFE TrustCrypt Module has the following physical dimensions:

- Size:
- Width 90mm
- Height 10mm
- Depth 60mm
- Maximum Weight: 100g

## *4.2 Cryptographic Module Boundary*

For FIPS 140-2 Level 3 validation the DigiSAFE TrustCrypt Module has been validated as a multi-chip embedded cryptographic module. Epoxy physically encloses the module HW/FW components and represents the cryptographic boundary of the module (see Figures 1a and 1b below). The epoxy has been tested to FIPS Level 3 Physical Security requirements including opacity and 'hardness'.

## *4.3 Physical Security Mechanisms*

The multi-chip embedded cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque epoxy enclosure.
- Hard potting material encapsulation of multiple chip circuitry enclosure with removal/penetration attempts causing serious damage.

## *4.4 Tamper Evidence Inspection*

The operator of the module shall periodically inspect all surfaces of the module for signs of tampering. The operator shall look out for scratches, drilling and cracks on all the surfaces.

The recommended interval for such inspection is at least once every 6 months.

## *4.5 Ports and Interfaces*

The DigiSAFE TrustCrypt's physical interfaces consist of several pins that support data input, data output, control input, and status output. The module has a total of 80 pins that cross its physical boundary. Ten of these pins are active and are considered the ports into and out of the cryptographic module.

The inactive pins that cross the physical boundary of the module are provided for latent functionality and can only be used by a customized application, which is out of scope of this validation. Pins that are reserved for future use are disabled and inactivated by the module and are made to float so that no signals can be input or output from them. Note that the active UART2 Tx pin (below) is disabled during error or alarm states in the same fashion to prevent any sensitive data from being output during those states.

- UART 2 Rx 1 pin (control input, data input)
- UART 2 Tx 1 pin (status output, data output)
- GPIO 3 pins (1 control input, 2 status output):
  - Config Type Pin – On Power up, this pin is used to check whether it is in Field Config Mode, Factory Config Mode or Operational Mode.
  - Field Config Pin - On power up when this pin is shorted with the Config Type Pin:
    - When the module's Key Encryption Key (KEK) is found inside the module but the CO & Users Passwords are not found inside the module, the module will enter the Initialize Password state. Note that password entry into the module is protected by the Key Encryption Key.
    - When the module's Key Encryption Key (KEK) and all Passwords are found inside the module, the module will enter the Crypto Officer Log In state. Note that Crypto Officer Login password entry is protected by the Key Encryption Key.
  - Factory Config Pin – On power up when this pin is shorted with the Config Type Pin, the module will enter the Key Encryption Key download state. This operation is performed in the manufacturing environment and is protected by the Key Encryption Key Publishing Authority private key which only the ST Electronics factory knows.
- GPIO External Tamper 1 pin (Control in - controls zeroization of SRAM)
- Vin 1 pin (Power in – 5.0V main power source)
- VBatt 1 pin (Power in - external 3.0V backup battery source to maintain the SRAM contents, RTC, and anti-tamper circuit when the main power is off)
- VRtc 1 pin (Power out – 3.3/3.0V derived from Vin and Vbatt, whichever is present)
- GND 1 pin (Power in/out – Electrical Ground)

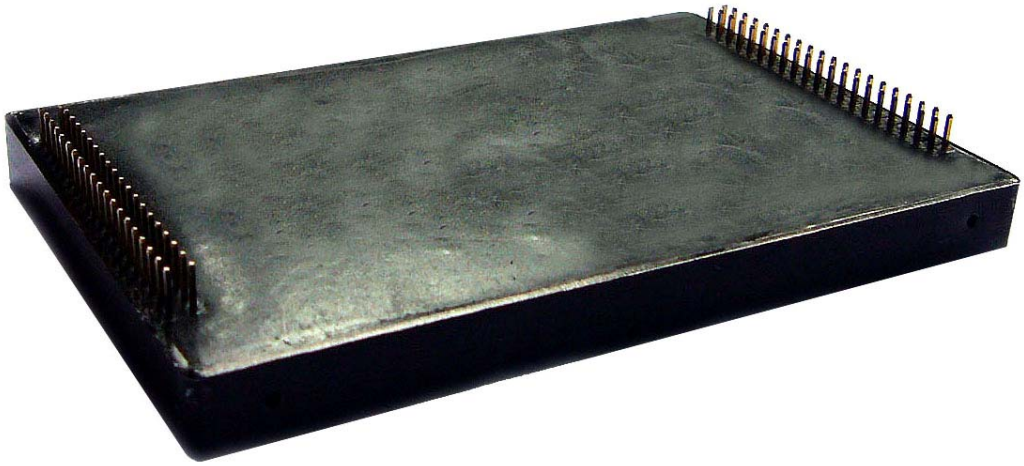

**Figure 1a – Image of the bottom of the Cryptographic Module**

**Figure 1b – Image of the top of the Cryptographic Module**

# 5. Identification and Authentication Policy

## *5.1 Assumption of Roles*

The cryptographic module shall support two distinct operator roles (User and Crypto-Officer). The cryptographic module shall enforce the separation of roles using identity-based operator authentication. An operator must enter an ID and its Password to log in. The ID is an alphanumeric string of exactly eight characters. The password is an alphanumeric string of exactly eight characters chosen from the 62 printable and human-readable characters. Authentications are cleared when power cycling the module, and operators must reauthenticate when power is reapplied.

**Table 2 - Roles and Required Identification and Authentication**

| Role | Type of Authentication | Authentication Data |
|---|---|---|
| User | Identity-based operator authentication | ID and Password |
| Crypto-Officer (CO) | Identity-based operator authentication | ID and Password |

**Table 3 – Strengths of Authentication Mechanisms**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| ID and Password | The probability that a random attempt will succeed or a false acceptance will occur is $1/62^8$ which is less than 1/1,000,000.<br>The probability of successfully authenticating to the module within one minute is $12/62^8$ which is less than 1/100,000. After every failed authentication attempt the module waits 5 seconds before it allows the next authentication attempt – therefore only a maximum of 12 authentication attempts can be made in one minute. |

# 6. Access Control Policy

## *6.1 Crypto-Officer Role*

This role represents the Crypto-Officer who authenticates via an ID/Password combination through UART2 (Tx Pin and Rx Pin). Table 4 lists all the services available to the Crypto-Officer, the service inputs & outputs, and the CSPs & Public keys accessed by each service.

**Table 4 – Crypto-Officer Services and Key/CSP Modes of Access**

| Service | Description | Input | Output | CSP & Public Key Access |
|---|---|---|---|---|
| Operator Authentication | Allows operator to enter the ID and password to login. The module checks these entered values against stored values. If the comparison is successful, then the appropriate role (CO) is assumed. | Crypto-Officer ID, Crypto-Officer Password (both AES Key Wrapped with KEK) | N/A | Read Crypto-Officer Password.<br>Read KEK. |
| Load App PA Public Key | Allows the CO to load the Application Publishing Authority Public Key (App PA Public Key). | App PA Public Key (AES Key Wrapped with KEK) | N/A | Write App PA Public Key. |
| Zeroize | Zeroizes all plaintext CSPs in the module.<br>Zeroizes plaintext Public Keys in the module.<br>Zeroizes the customized application (if one is currently loaded in FLASH).<br>Zeroizes all contents stored in SRAM.<br>The module enters an endless loop after zeroization - all data output is stopped, all data input is ignored, a zeroized status packet is output every minute.<br>After zeroization the module must be sent back to the factory to become operational again. | N/A | N/A | Zeroize:<br>• Key Encryption Key (KEK).<br>• User Data Secret Key (immediately after use).<br>• User Data Private Key (immediately after use).<br>• Crypto-Officer Password.<br>• User Password.<br>• App PA Public Key.<br>• User Data Public Key (immediately after use). |
| Load Customized Application | Allows the CO to enter a signed customized application. | Signed customized application | N/A | Read App PA Public Key. |
| Update Crypto-Officer Password | Allows the CO to update the Crypto-Officer Password. | Crypto-Officer ID, Crypto-Officer Password (both AES Key Wrapped with KEK) | N/A | Write Crypto-Officer Password. |

| Service | Description | Input | Output | CSP & Public Key Access |
|---|---|---|---|---|
| Update User Password | Allows the CO to update the User Password. | User ID, User Password (both AES Key Wrapped with KEK) | N/A | Write User Password. |

## *6.2 User Role*

This role represents the User who authenticates via an ID/Password combination through UART2 (Tx Pin and Rx Pin). Table 5 lists all the services available to the User, the service inputs & outputs, and the CSPs & Public keys accessed by each service.

**Table 5 – User Services and Key/CSP Modes of Access**

| Service | Description | Input | Output | CSP Access |
|---|---|---|---|---|
| Operator Authentication | Allows operator to enter the ID and password to login. The module checks these entered values against stored values. If the comparison is successful, then the appropriate role (User) is assumed. | User ID, User Password (both AES Key Wrapped with KEK). | N/A | Read User Password.<br>Read KEK. |
| Encrypt Data | Allows the User to encrypt a payload. Refer to Table 7 for available ciphers. | Payload to be encrypted.<br>User Data Secret Key (AES Key Wrapped with KEK). | Encrypted Payload. | Read User Data Secret Key.<br>Read KEK.<br>Zeroize User Data Secret Key. |
| Decrypt Data | Allows the User to decrypt a payload. Refer to Table 7 for available ciphers. | Payload to be decrypted.<br>User Data Secret Key (AES Key Wrapped with KEK). | Decrypted Payload. | Read User Data Secret Key.<br>Read KEK.<br>Zeroize User Data Secret Key. |
| Sign Data | Allows the User to sign a payload. Refer to Table 7 for available ciphers. | Payload to be signed.<br>User Data Private Key (AES Key Wrapped with KEK). | Signature for payload. | Read User Data Private Key.<br>Read KEK.<br>Zeroize User Data Private Key. |
| Hash Data | Allows the User to hash a payload. Refer to Table 7 for available ciphers. | Payload to be hashed. | Hash of payload. | N/A |
| Verify Signature | Allows the User to verify a signature. Refer to Table 7 for available ciphers. | Signed Payload.<br>User Data Public Key (AES Key Wrapped with KEK). | Boolean: 'yes' if signature matches, otherwise 'no' | Read User Data Public Key.<br>Read KEK.<br>Zeroize User Data Public Key. |
| Get Deterministic Random Number | Allows the User to retrieve a random number from the module's approved DRNG. | Random number length. | Random number. | N/A |
| Get Non-Deterministic Random Number | Allows the User to retrieve a random number from the Hardware RNG. | Random number length. | Random number. | N/A |
| Update User Password | Allows the User to update the User Password | User ID, User Password (both AES Key Wrapped with KEK). | N/A | Write User Password.<br>Read KEK. |

## *6.3 Unauthenticated Services*

The following services do not require authentication prior to invocation, they are available through UART2 (Tx Pin and Rx Pin).

**Table 6 – Services Available without Assuming a Role**

| Service | Description | Input | Output | CSP Access |
|---|---|---|---|---|
| Show Status | Alerts the operator of the status of the module.<br><br>On power-up the module will output a Power Up System Information status packet containing the module's version, release date, and bootstrap application & crypto library checksum.<br><br>After power-up self-tests are run the module will output a Power Up Self Test Results status packet containing pass/fail codes for each of the power-up self-tests.<br><br>Each time the module enters major FIPS states it will output a state status packet.<br><br>While in the Fatal Error State the module will output a PKT_STATE _ERROR state packet once every minute.<br><br>At the conclusion of processing each service request the module returns a status results code. | N/A | Status of module. | N/A |
| Power Up Self Test | This allows an operator to perform the power up self tests by power cycling the module. | N/A | Pass/Fail for each of the self-tests. | N/A |
| Zeroize SRAM | This allows the host system to zeroize all contents stored in the module's SRAM. Activated via the module's GPIO External Tamper pin. | N/A | N/A | N/A.<br>The SRAM is meant to store security parameters by customized application |

# 7. Cryptographic Keys and CSPs

**Table 7 – Available Ciphers**

| Encryption Ciphers | Decryption Ciphers | Signature Ciphers | Hash Ciphers | RNG |
|---|---|---|---|---|
| AES 128 ECB<br>AES 128 CBC<br>AES 128 CFB<br>AES 128 OFB<br>AES 192 ECB<br>AES 192 CBC<br>AES 192 CFB<br>AES 192 OFB<br>AES 256 ECB<br>AES 256 CBC<br>AES 256 CFB<br>AES 256 OFB | AES 128 ECB<br>AES 128 CBC<br>AES 128 CFB<br>AES 128 OFB<br>AES 192 ECB<br>AES 192 CBC<br>AES 192 CFB<br>AES 192 OFB<br>AES 256 ECB<br>AES 256 CBC<br>AES 256 CFB<br>AES 256 OFB | RSA 1024<br>RSA 2048 | SHA-256<br>SHA-512 | ANSI X9.31 DRNG<br>Hardware NDRNG |

**Table 8 – Secret and Private Keys**

| Key | Description/Usage | Generation | Storage | Entry/Output | Destruction |
|---|---|---|---|---|---|
| **Key Encryption Key (KEK)** | This is an AES 256-bit key that is used to decrypt all the following when they are entered into the module: User Data Secret Keys, User Data Private Keys, the App PA Public Key, User Data Public Keys, the CO Officer ID & Password, and the User ID & Password. | Generated externally. | Stored in plaintext in FLASH. | Entry: The KEK is entered into the module during manufacturing.<br><br>Output: N/A | Zeroized when the zeroize service is invoked. |
| **User Data Secret Key (UDSK)** | This is an AES 256-bit, AES 192-bit, or AES 128-bit key that is used to encrypt or decrypt bulk operator supplied data. | Generated externally. | Stored in plaintext in DRAM. | Entry: The UDSK is entered in encrypted form (AES Key Wrapped with KEK).<br><br>Output: N/A | Zeroized immediately after use. |
| **User Data Private Key (UDPK)** | This is an RSA 1024-bit, or 2048-bit private key that is used to sign bulk operator supplied data. | Generated externally. | Stored in plaintext in DRAM. | Entry: The UDPK is entered in encrypted form (AES Key Wrapped with KEK).<br><br>Output: N/A | Zeroized immediately after use. |

**Table 9 – Public Keys**

| Key | Description/Usage | Generation | Storage | Entry/Output |
|---|---|---|---|---|
| **KEK PA Public Key** | RSA 2048-bit public key used in manufacturing during KEK download to verify the signature over the KEK. | Generated externally. | Stored in plaintext in FLASH. | Entry: Loaded in plaintext during manufacturing.<br><br>Output: N/A |
| **App PA Public Key** | RSA 2048-bit public key used to authenticate customized applications. | Generated externally. | Stored in plaintext in FLASH. | Entry: Entered by Crypto-Officer in encrypted form (AES Key Wrapped with KEK).<br><br>Output: N/A |
| **User Data Public Key** | RSA 1024-bit, or 2048-bit public key used to verify operator supplied signatures. | Generated externally. | Stored in plaintext in DRAM. | Entry: Entered in encrypted form (AES Key Wrapped with KEK).<br><br>Output: N/A |

**Table 10 – Other CSPs**

| Key | Description/Usage | Generation | Storage | Entry/Output | Destruction |
|---|---|---|---|---|---|
| **Cryptographic Officer Password** | This is the password that is used to authenticate the CO.<br><br>The password policy is:<br><br>- Exactly 8 characters<br><br>- 62 possible alpha / numeric character set. | Generated externally. | Stored in plaintext in FLASH. | Entry: Entered via the Operator Authentication service and updated via the Update Crypto-Officer ID / Password service. Entered each time the CO authenticates to the module. Whenever this CSP is entered into the module it is encrypted with the KEK (AES256 Key Wrapping).<br>Output: N/A | Zeroized when the zeroize service is invoked. |
| **User Password** | This is the password that is used to authenticate the User.<br><br>The password policy is:<br>- Exactly 8 characters<br><br>- 62 possible alpha / numeric character set. | Generated externally. | Stored in plaintext in FLASH. | Entry: Entered via the Operator Authentication service and updated via the Update User ID / Password service. Entered each time the User authenticates to the module. Whenever this CSP is entered into the module it is encrypted with the KEK (AES256 Key Wrapping).<br>Output: N/A | Zeroized when the zeroize service is invoked. |

# 8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the cryptographic module does not contain a modifiable operational environment.

# 9. Security Rules

The module's design corresponds to the following security rules. These rules are enforced by the module to implement the security requirements of FIPS 140-2 Level 3 modules.

1. The cryptographic module provides two distinct roles. These are the User role, and the Crypto-Officer role.
2. The cryptographic module provides identity-based authentication.
3. When the module has not been placed in an authenticated role, the operator does not have access to any cryptographic services.
4. The cryptographic module performs the following tests:
   A. Power up Self-Tests:

   **Cryptographic Algorithm Tests**

   1. AES-256 ECB Mode KAT
   2. SHA-256 KAT
   3. SHA-512 KAT
   4. RSA-1024 KAT Sig Gen & Sig Verify
   5. RSA-2048 KAT Sig Gen & Sig Verify
   6. ANSI X9.31 RNG KAT

   **Software/Firmware Integrity Test**

   1. 16-bit Firmware Integrity Test (EDC)

   B. Conditional Self-Tests:

   **Continuous RNG Tests**

   1. RNG Every generation of 128 bits of random data from the RNG will be compared with the previous 128 bits to ensure that they are not equal.
   2. NDRNG Every generation of 128 bits of random data from the NDRNG will be compared with the previous 128 bits to ensure that they are not equal.

   C. Vendor Defined Critical Function Tests:
      1. Load Custom Application - Signature Verification Test (RSA 2048-bit Verification)
5. At any time the operator can command the module to perform the power-up self-tests by power cycling the module.
6. Prior to each use, the internal RNGs are tested using the continuous RNG test.
7. Data output is inhibited during self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module does not support concurrent operators.

10. The module does not support a maintenance interface or a maintenance role.

11. The module does not support Bypass functionality.

12. The module does not support the generation of cryptographic keys.

13. The module does not support the output of CSPs.

14. The seed Key and seed value for the RNG (ANSI X9.31) are read from the onboard NDRNG during power up. They are compared to ensure that they are not equal.

This section documents the security rules imposed by the vendor:

1. After every failed authentication attempt the module waits 5 seconds before it allows the next authentication attempt – therefore only a maximum of 12 authentication attempts can be made in one minute.
2. After zeroization the module must be returned to the factory to become operational again (download the KEK back into the module).
3. The module supports an external GPIO pin that allows complete zeroization of SRAM. This allows host systems that contain the module to zeroize all contents within SRAM by activating the GPIO pin.
4. Each module will be loaded with a unique, randomly generated KEK during manufacturing. ST Electronics will not monitor or record these KEK values.

# 10. Mitigation of Other Attacks Policy

FIPS 140-2 Area 11 Mitigation Of Other Attacks requirements are not applicable because the module is not designed to mitigate specific attacks beyond the current FIPS 140-2 requirements.

# 11. Definitions and Acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard |
| ANSI | American National Standards Institute |
| App PA | Application Publishing Authority Public Key |
| CBC | Cipher Block Chaining |
| CFB | Cipher Feedback |
| CO | Crypto-Officer |
| CSP | Critical Security Parameter |
| DRAM | Dynamic Random Access Memory |
| ECB | Electronic Codebook |
| EDC | Error Detection Code |
| GPIO | General Purpose Input/Output |
| KEK | Key Encryption Key |
| KEK PA | Key Encryption Key Publishing Authority |
| NDRNG | Non-Deterministic Random Number Generator |
| OFB | Output Feedback |
| PA | Publishing Authority |
| RNG | Random Number Generator |
| RSA | Rivest Shamir Adelman |
| SHA | Secure Hash Algorithm |
| SRAM | Static Random Access Memory |
| UART | Universal Asynchronous Receiver/Transmitter |