STSAFE-J100

Flexible programmable secure solution

Data brief

VQFN32

Features

- ECC support for NIST-P-256 and other curves are supported depending on the product
- Digital signature generation and verification with ECDSA
- Key agreement with Diffie-Hellman (ECKA-ECDH) and El Gamal (ECKA-EG)
- ECDH-GM primitive for PACE protocol
- On-chip RSA and ECC key pair generation
- Key pair, public key and PIN objects
- Up to 88.6 Kbytes of user memory
- Extended-length APDUs
- In-house personalization services
- Full ecosystem with expansion board and middleware
- Supports specific application loading
- Different ST applets available for preloading

Platform

- Java Card™ 3.0.4 Classic Edition
- GlobalPlatform® 2.1.1
- GlobalPlatform 2.2 - Amendment D - SCP03
- ISO/IEC 7816 T=0 and T=1 contact protocols
- Standard I^2C communication up to 100 kHz

Hardware

- Arm® SecurCore® SC000™ 32-bit RISC core
  - 30-year data retention at 25 °C
  - 500 000 erase/write cycles at 25 °C
- Operating temperature: –40 to +85 °C
- Enhanced NESCRYPT cryptoprocessor for public key cryptography
- Contact assignment compatible with ISO/IEC 7816-3 standards
- Asynchronous receiver transmitter (IART) for high speed serial data support (ISO/IEC 7816-3 and EMV® compliant)
- ESD protection greater than 6 kV (HBM) for contact pads
- 1.62 V to 5.5 V supply voltages
- ECOPACK® 32-lead VFQFPN 5×5 mm (0.5 mm pitch)

Security

- AIS-31 class PTG.2 compliant true random number generator (TRNG)
- AIS-20/31 class DRG.3 deterministic number generator (DRNG)
- Enhanced cryptographic algorithms:
  - DES/3DES, ECC and AES
  - SHA-1, SHA224, SHA-256, SHA384, SHA512, MD5 and CRC16
  - Generic Mapping primitive for Password Authenticated Connection Establishment (PACE) protocol
- Hardware security DES accelerator
- Hardware security AES
- Differential power analysis (DPA) and differential fault analysis (DFA) countermeasures against side-channel attacks
- Active shield
- Unique serial number on each die

Certifications

- Hardware IC Common Criteria certified EAL5+
  - Certificate ANSSI-CC-2015/59 with maintenance report ANSSI-CC-2015/59-M01
- Java Card Platform Common Criteria certification EAL5+ (AVA_VAN.5, ALC_DVS.2)
  - Reference PP: Java Card Closed Configuration Protection Profile, v3.0
  - Certificate ANSSI-CC-2017/23

Applications

Java Card/GlobalPlatform secure element providing authentication, data management and cryptographic services to customer's or ST’s embedded Java Card applications.

Contents

1 Description

The STSAFE-J100 is a highly secure solution based on an Arm®(a) SecurCore® SC000™ 32-bit RISC core. It acts as a secure element by providing authentication, data management and cryptographic services to a local or remote host.

The device embeds a secure Java Card operating system (3.0.4) compliant with GlobalPlatform (VGP 2.1.1 Configuration 2). It is ported on the latest generation of secure microcontrollers.

Combined with specific applications, the STSAFE-J100 addresses a very wide range of use cases. It can for instance be used for IoT (Internet of Things) devices, utilities, industrial applications and consumer electronics devices.

1.1 Development tools

ST provides a complete set of tools for the integration of the security module:

- STSAFE-J100 test tools
- Development board (reference: STS-J-PROGQ32xxx)

Note: Contact your local ST support office for available host software and drivers.

a. Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

1.2 Pin and signal description

Figure 1. VQFN32 pinout

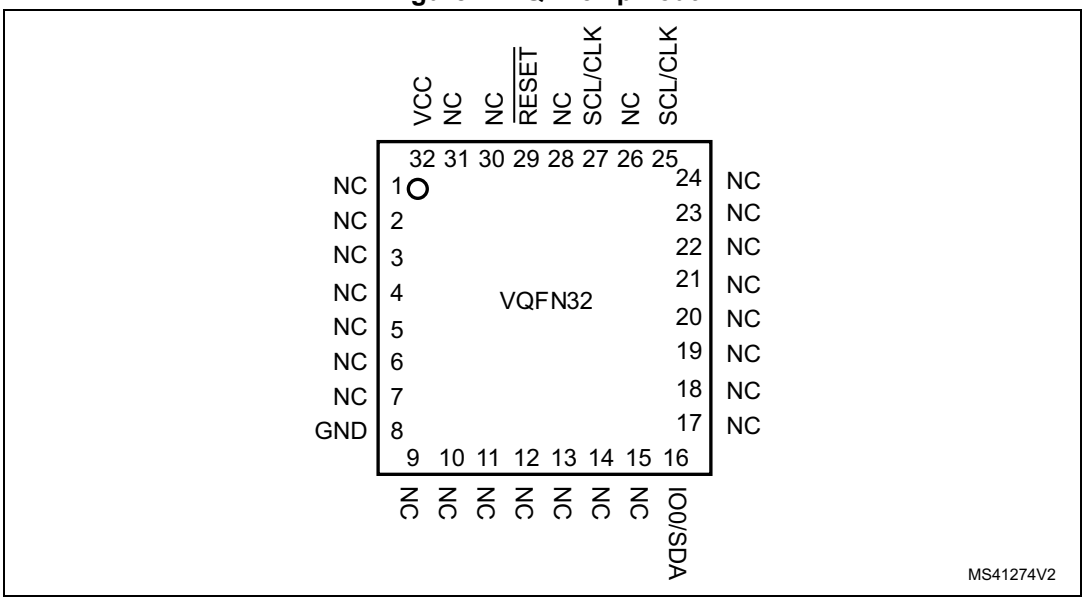


Table 1. Pin descriptions

Signal	Type	Description
GND	Input	GND has to be connected to the main motherboard ground.
$\overline{\text{RESET}}$	Input	Reset used to re-initialize the device
IO0/SDA	I/O	ISO 7816 IO0 pin or I2C serial data pin depending on the selected configuration (ISO or I2C)
VCC	Power	Power supply pin
SCL/CLK	Input	ISO 7816 clock pin or I2C clock pin(1) depending on the selected configuration (ISO or I2C)

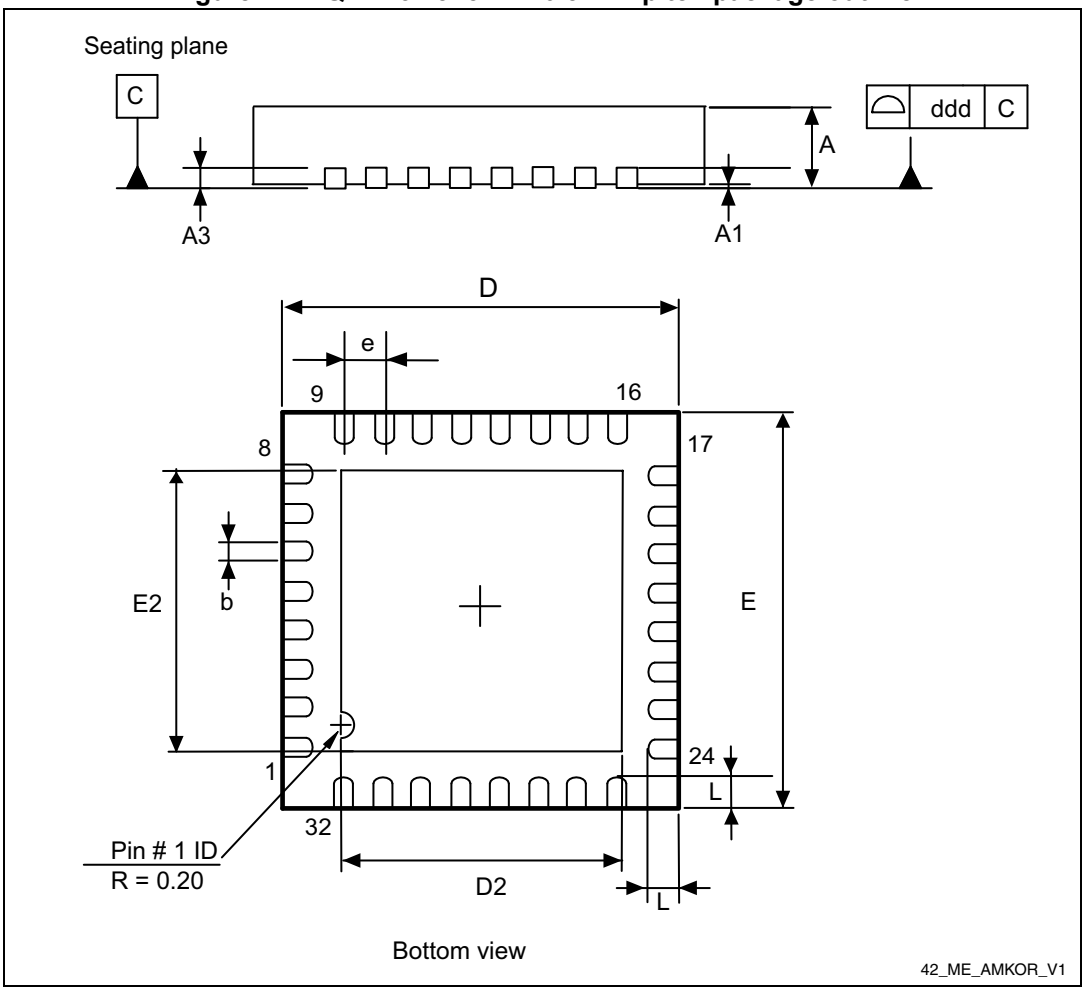
1. Pin 27 and pin 25 are connected internally.

2 Package information

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.

2.1 32-lead very thin fine pitch quad flat pack no-lead (VFQFPN) package information

Figure 2. VFQFPN32 5×5 mm 0.5 mm pitch package outline



1. Drawing is not to scale.

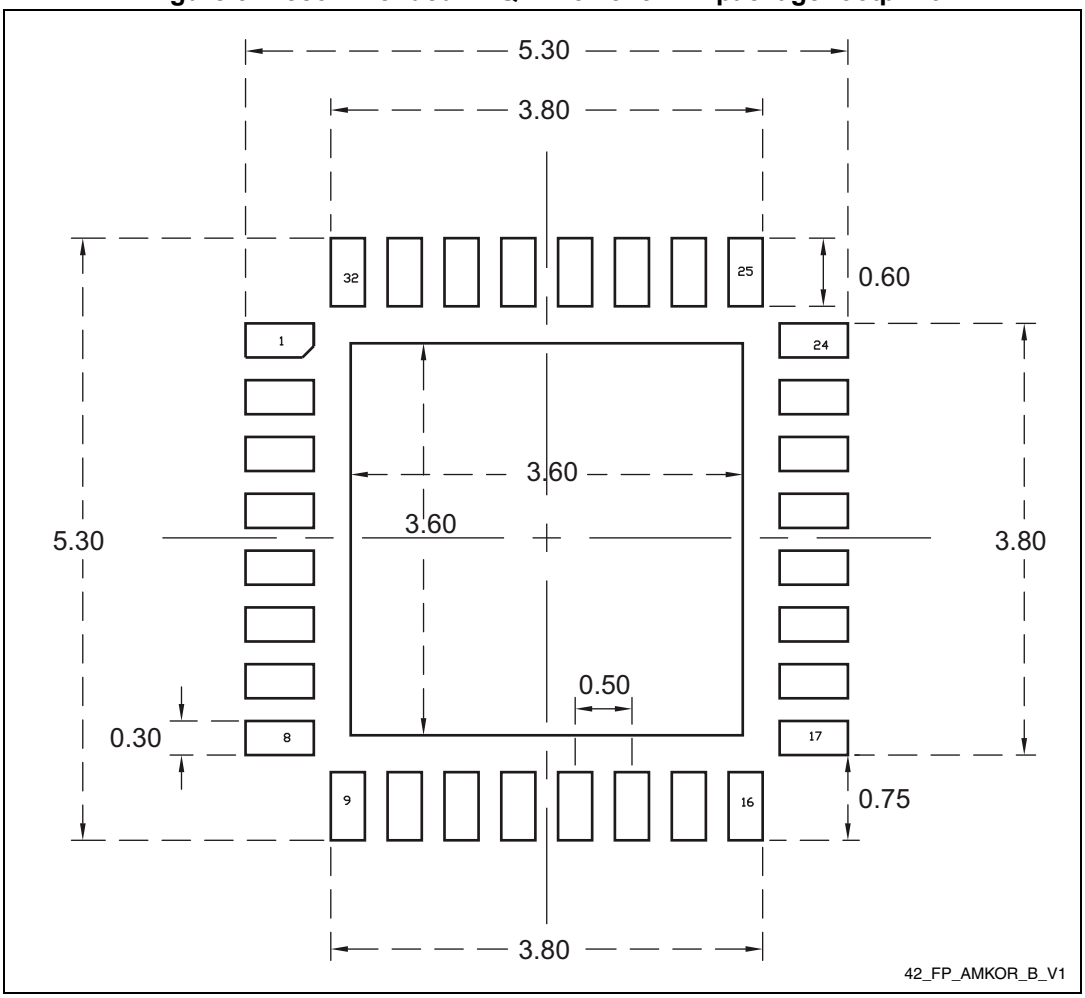
Table 2. VFQFPN32 5×5 mm package mechanical data

Symbol	millimeters			inches [1]		
	Min	Typ	Max	Min	Typ	Max
A	0.800	0.900	1.000	0.0315	0.0354	0.0394
A1	0.000	0.020	0.050	0.0000	0.0008	0.0020
A3	-	0.200	-	-	0.0079	-
b	0.180	0.250	0.300	0.0071	0.0098	0.0118
D	4.850	5.000	5.150	0.1909	0.1969	0.2028
D2	3.500	3.600	3.700	0.1378	0.1417	0.1457
E	4.850	5.000	5.150	0.1909	0.1969	0.2028
E2	3.500	3.600	3.700	0.1378	0.1417	0.1457
e	-	0.500	-	-	0.0197	-
L	0.300	0.400	0.500	0.0118	0.0157	0.0197
ddd	0.050			0.0020		

1. Values in inches are converted from mm and rounded to 4 decimal digits.

2.2 Recommended footprint

Figure 3. Recommended VFQFPN32 5×5 mm package footprint



1. All dimensions in millimeters.

3 Revision history

Table 3. Document revision history

Date	Revision	Changes
29-Jul-2016	1	Initial release.
05-Oct-2016	2	Updated *Section 1: Description*.
17-Apr-2018	3	Updated user memory size, list of supported enhanced cryptographic algorithms and ambient operating temperature range. Updated certification information. Added Arm logo and trademark notice. Small text changes.