ST4SIM-110S

Data brief

SIM system-on-chip solution for secure IoT applications

Card plugin 2FF, 3FF or 4FF (based on D18 micromodule

Card plugin with triple cut (based on D18 micromodule)

Product status link
ST4SIM-110S

Features

- Configurable cellular network connectivity by a trusted partner
- Compliant with 2G / 3G / 4G (LTE) / CDMA / NB-IoT / CAT–M networks
- Network access applications supported: SIM / USIM / ISIM / CSIM
- Secure element access control (ARF / PKCS#15)
- OTA capability over SMS, CAT-TP & HTTPS (including DNS)

Hardware

- Product available on ST33G1M2
- ST33 product based on a 32-bit Arm® SecurCore® SC300™ RISC core
- Supply voltage: Class A (5 V), Class B (3 V), Class C (1.8 V)
- Asynchronous serial I/O port ISO/IEC 7816-3 compatible (T=0 protocol)
- Operating temperature: -25°C to +85°C
- Common Criteria EAL5+

ECOPACK-compliant packages

- 2FF, 3FF or 4FF plugin card (based on D18 micromodule)
- Triple cut plugin card (based on D18 micromodule)

Security

- Symmetric cryptography DES / 3DES / AES
- Asymmetric cryptography RSA (up to 2048 bits)
- HTTPS remote management TLS v1.0, v1.1 and v1.2
- Elliptic curve cryptography (up to 521 bits) including preloaded curve NIST P-256 and brainpool P256r1
- Authentication algorithm: MILENAGE, TUAK, CAVE

Software standard compliance

- Java® Card v3.0.4 Classic
- GlobalPlatform® card specification v2.2, including GP amendments A, B, C, D and E
- ETSI, 3GPP and 3GPP2 release 12 (for further information, contact the local STMicroelectronics sales office)
- Power saving features (PSM and eDRX) defined by ETSI release 13

Applications

- Cellular Connected Nodes
- LTE: Cat M1 and NBIoT
- Surveillance
- IoT for smart home and city

1 Description

The ST4SIM-110S is an STMicroelectronics SIM and embedded SIM (eSIM or eUICC) product designed for IoT devices.

The ST4SIM-110S pre-integrates a cellular connectivity configuration provided by trusted partners. In this way, the product is ready to be deployed to the field.

The device ensures the appropriate security level to all eSIM stakeholders (user, MNO, OEM, hardware integrator, service provider, and so on).

The device can include an embedded secure element to store credentials and/or independent applications directly managed by the MCU (or by another OEM element).

The device provides a secure and interoperable Java® Card environment compliant with Java® Card v3.0.4 classic. Moreover, the device integrates the most advanced UICC features compliant with GlobalPlatform®, ETSI, 3GPP, 3GPP2 specifications.

The device integrates a dynamic memory management with Java® Card garbage collection mechanism optimizing the usage of the memory.

The device is based on the ST33G1M2, an industrial grade hardware solution (JEDEC) supporting severe conditions. This solution is a tamper-resistant secure element certified by Common Criteria EAL5+, with a powerful 32-bit Arm® SecurCore® SC300™ RISC core.

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

Note: Java is a registered trademark of Oracle and/or its affiliates.

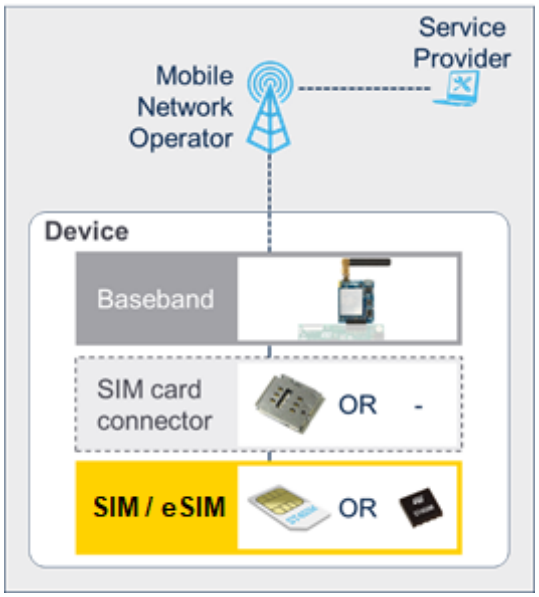
2 Cellular connectivity solutions overview

A cellular connectivity solution enables devices to be used by the edge mobile network operators (also called MNO) or mobile virtual network operators (MVNO). This solution increases network coverage and it maintains seamless connectivity.

Moreover, a cellular solution is simple to deploy. This solution is mainly composed of the modem (baseband), the SIM card connector and the plastic SIM card. This is the traditional SIM concept inherited from the mobile phone.

It is also possible to have an embedded SIM (eSIM) solution. In this case, there is no SIM card connector. In this case, there is no SIM card connector. It reduces the board footprint and there is no need for a SIM connector.

Figure 1. SIM and eSIM architecture overview



3 Card OS technical features

3.1 Supported standards and networks

The ST4SIM-110S solution complies with the standard networks (2G / 3G / 4G LTE) and low power networks (CAT-M / NB-IoT).

From a technical point of view, the ST4SIM-110S solution integrates all advanced NAAs for eSIM solution:

- USIM applications providing access to universal mobile telecommunications system (UMTS) networks,
- IP multimedia services identity module (ISIM) to access IP multimedia subsystem (IMS) networks,
- CDMA subscriber identity module (CSIM) including CAVE algorithm.

To grant mobile network operators (MNO) the best solution for UICC-centric services either owned by the MNO or by third parties, the ST4SIM-110S complies with GlobalPlatform® Card Specifications v2.2 (depending on UICC configuration) and related amendments.

3.2 Algorithms and cryptography

The ST4SIM-110S supports the following standard authentication algorithms:

- CAVE
- MILENAGE
- TUAK

The MILENAGE algorithm enables authorized access to UMTS/LTE networks with an easy and flexible parameter customization, according to specific MNO requirements.

The TUAK authentication algorithm is supported with both 128-bit key length and 256-bit key length.

In addition to these algorithms, the ST4SIM-110S also supports the "3GPP test algorithm" for test profiles.

In order to increase security performance, the ST4SIM-110S also incorporates a ratification counter that limits the number of authentication attempts to prevent brute-force attacks designed to break algorithms. In addition, all algorithms support dedicated DPA/SPA attack countermeasures.

Besides standard symmetric cryptography and hashing algorithms (DES, Triple DES, AES, MD5, and so on), the ST4SIM-110S provides a cryptographic co-processor with asymmetric cryptography capabilities.

For applications requiring the strongest level of cryptography, the ST4SIM-110S supports:

- RSA with a key length of up to 2048 bits
- elliptic curve cryptography (ECC) with a key length of up to 521 bits.

In addition, the ST4SIM-110S fully supports the PKCS#15 standard and offers a rule-based access control mechanism such as digital signature/certificates for data/applications requiring a strong level of cryptography.

The security algorithm implementation adheres to the chip security guidelines of the ST33G1M2 to guarantee the best security level (for more information, contact the local STMicroelectronics sales office).

3.3 Over the air (OTA) functionality

The ST4SIM-110S supports over the air protocol for remote application management (RAM) and remote file management (RFM) compliant with ETSI standard (ETSI TS 102 225 and ETSI TS 102 226 specifications Release 12).

The RAM application is also fully supported by GlobalPlatform v2.2 and the related amendment B (which enables remote applet management and remote file management over HTTP/TLS).

TLS v1.0, 1.1 and 1.2 are available in the ST4SIM-110S. In addition, the ST4SIM-110S integrates a DNS mechanism allowing the card to request the HTTPS server address from a DNS server.

The ST4SIM-110S is able to remotely control the execution of APDU commands over the air, to administrate the card content. It also allows proactive commands to interact with the host device.

The ST4SIM-110S supports the secured packet structure and the remote APDU structure for (U)SIM toolkit applications, conforming 3GPP TS 31.115 and TS 31.116 specifications.

The CAT-TP protocol defined by ETSI release 7 is supported.

As it is compliant with the ETSI, 3GPP and 3GPP2, the ST4SIM-110S can easily be integrated into any OTA platform compliant with relevant standards. STMicroelectronics cards are field-proven to be interoperable with the mainstream OTA platforms commonly chosen by mobile network operators.

3.4 Memory management

The OTA mechanism includes the support of 3G UICC administrative commands as specified by ETSI TS 102 222.

These commands are integrated by a powerful dynamic memory management that allows complete smart memory defragmentation.

Dynamic memory management provides:

- Common space for files, packages, applets and objects
- Memory recovery on deletion operations
- Total free memory available in the select MF response.

The OTA mechanism is designed to allow a very fast and silent memory recovery, absolutely safe for the end user data.

The ST4SIM-110S is capable of enhancing intrinsic Flash memory cells for files requiring intense update and high reliability.

Memory quota mechanism based on the GlobalPlatform Amendment C (CGM) is supported. The mechanism can be disabled at card configuration.

4 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.

4.1 Card plugin package information

The ST4SIM-110S card is based on flexible plastic chip cards, composed of ABS and PVC. This card contains a STMicroelectronics D18 micromodule.

All elements; card and micromodule, are designed to run at a temperature of -25°C to +85°C.

The ST4SIM-110S is available for different card plugin packages as detailed in the table below.

Table 1. SIM plugin package types and dimensions

Package	3 in 1 SIM (Triple Cut)	Mini SIM (2FF)	Micro SIM (3FF)	Nano SIM (4FF)
Package format				
Height	25 mm (±0.1 mm)	25 mm (±0.1 mm)	15 mm (±0.1 mm)	12.3 mm (±0.1 mm)
Width	15 mm (±0.1 mm)	15 mm (±0.1 mm)	12 mm (±0.1 mm)	8.8 mm (±0.1 mm)
Thickness	0.76 mm (±0.08 mm)	0.76 mm (±0.08 mm)	0.76 mm (±0.08 mm)	0.67 mm (±0.03 / -0.07 mm)

Note: These formats comply to the ISO/IEC 7810 and ETSI TS 102 221 standards.

4.1.1 D18 micromodule pinout information

The contact of D18 micromodule are compliant with ISO/IEC 7816 and ETSI TS 102 221 standard. The contact assignment layout is given in the figure below and contact description is in the following table.

Figure 2. D18 micromodule contact assignment

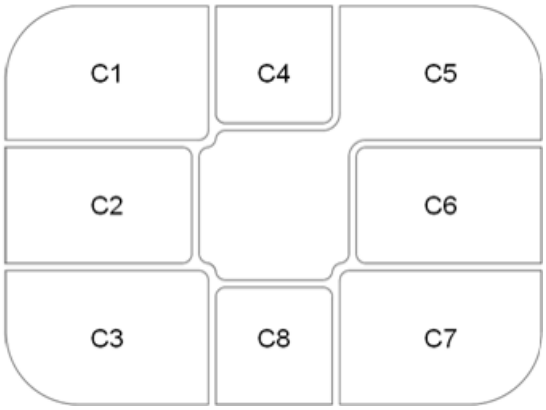


Table 2. D18 contact descriptions

Name	Contact number	Description
VCC	C1	Power supply
ISO_RST/GPIO5	C2	ISO 7816-3 interface reset
ISO_CLK/GPIO6	C3	ISO 7816-3 interface CLK
Reserved for future use	C4	Not used
GND	C5	Ground supply
SWIO	C6	Not used
ISO_IO0/GPIO7	C7	ISO 7816-3 interface serial input/output
Reserved for future use	C8	Not used

5 Acronyms and abbreviations

Table 3. **Glossary**

Term	Description
3GPP	3rd Generation Partnership Project
AES	Advanced encryption standard
AID	Application identifier
APDU	Application protocol data unit
ARF	Access rule file
ASN.1	Abstract syntax notation 1
CAT-M	LTE card application toolkit (CAT) M
CAT-TP	Card application toolkit transport protocol
CAVE	Cellular authentication and voice encryption
CDMA	Code division multiple access
CSIM	CDMA subscriber identity module
DES	Data encryption standard
DFN	Dual flat no-lead package
DNS	Domain name server
EAL	Evaluation assurance level
eDRX	Extended discontinuous reception
eSE	Embedded secure element
eSIM	Embedded SIM
ETSI	European Telecommunications Standards Institute
eUICC	Embedded Universal integrated circuit card
HTTPS	Secured HTTP
IEC	International electrotechnical commission
IMS	IP multimedia service or IP Multimedia Core Network Subsystem (IMS) is an architectural framework for delivering IP multimedia services
IoT	Internet of things
ISO	International organization for standardization
ISIM	IP multimedia services identity module
JEDEC	Joint electron device engineering council (semiconductor engineering standardization)
LTE	Long-term evolution
M2M	Machine to machine
MD5	The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value
MNO	Mobile network operator
NAA	Network access application
NB-IoT	Narrow band Internet of Things
NIST	National Institute of Standards and Technology
NMI	Non-maskable interrupt
OEM	Original equipment manufacturer

Term	Description
OTA	Over the air
PIN	Personal identification number
PKCS	Public key cryptographic standards
PoC	Proof of concept
PUK	PIN unlock key
RAM	Remote application management
RFM	Remote file management
RISC	Reduced instruction set computer
RSA	Ron Rivest, Adi Shamir and Leonard Adleman Public-key cryptosystem
SCP	Secure channel protocol
SE	Secure element
SIM	Subscriber identity module
SM-DP	Subscription manager - data preparation
SM-SR	Subscription manager - Secure routing
SMS	Simple message system
TAR	Toolkit application reference
TLS	Transport layer security
UICC	Universal integrated circuit card
UMTS	Universal mobile telecommunications systems
USIM	Universal subscriber identity module

Revision history

Table 4. **Document revision history**

Date	Version	Changes
20-Jan-2021	1	Initial release.

Contents

List of tables

List of figures