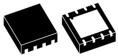
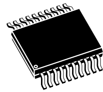
SIM and eSIM system-on-chip solution for secure automotive applications

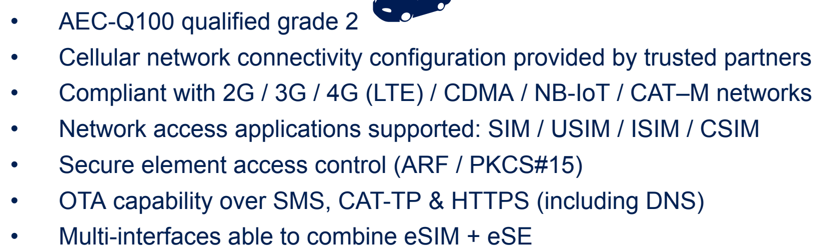


VFDFPN8
5 × 6 mm,
Wettable flanks
(MFF2)



TSSOP20
6.5 × 4.4 mm

Features



- AEC-Q100 qualified grade 2
- Cellular network connectivity configuration provided by trusted partners
- 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)
- Multi-interfaces able to combine eSIM + eSE

Hardware

- Product available on ST33G1M2A
- 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)
- Serial peripheral interface (SPI), depending on packages
- Automotive qualification (AEC-Q100 qualified grade 2)
- Operating temperature: -40°C to +105°C
- Common Criteria EAL5+

ECOPACK-compliant packages

- VFDFPN8 5 × 6 mm, wettable flank (MFF2)
- TSSOP20 6.5 × 4.4 mm

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

Product status link
ST4SIM-110A

Applications

- Emergency call (eCall)
- Infotainment head unit
- Cellular Connected Nodes
- LTE: Cat M1 and NBIoT
- Surveillance

1 Description

The ST4SIM-110A is an STMicroelectronics SIM and embedded SIM (eSIM or eUICC) product designed for the automotive market.

The ST4SIM-110A 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 ST33G1M2A, an automotive grade hardware solution, AEC-Q100 qualified grade 2 supporting extreme 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.

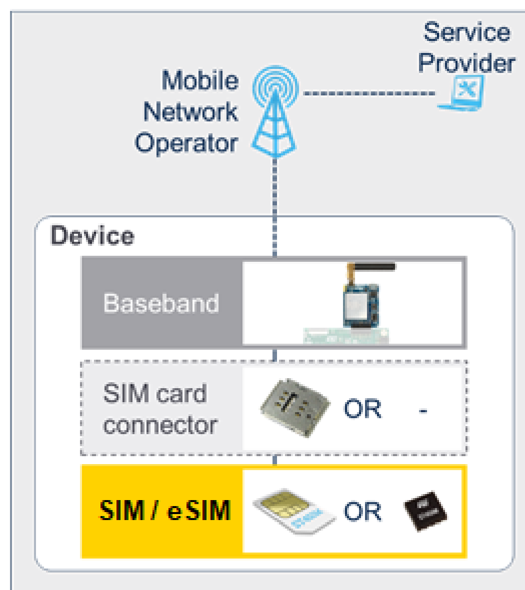
2 Cellular connectivity solutions overview

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. It reduces the board footprint and there is no need for a SIM connector.

Figure 1. SIM and eSIM architecture overview

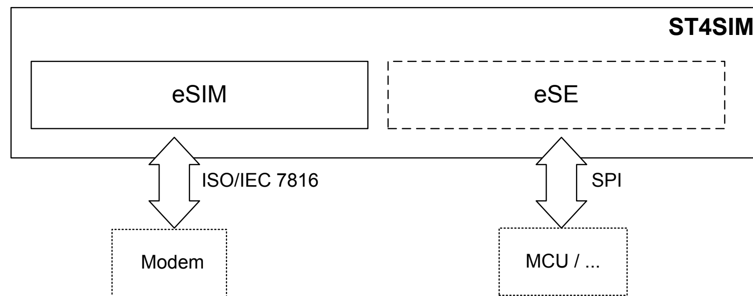


3 Additional embedded secure element (eSE)

The ST4SIM-110A is able to combine the eSIM solution with an embedded secure element (eSE) section inside the same chip.

This eSE section is used to provide secure storage, cryptographic services, and so on via Java® Card applets.

Figure 2. ST4SIM-110A architecture eSIM & eSE overview



The eSE section is accessible through a dedicated serial peripheral interface (SPI) protocol and the eSIM uses the ISO/IEC 7816 protocol in parallel. Consequently, the eSE is only available on TSSOP20 packages including ISO and SPI protocols.

The embedded secure element is optional and configurable.

Contact the local STMicroelectronics sales office for more details on the pin configuration.

4 Card OS technical features

4.1 Supported standards and networks

The ST4SIM-110A 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-110A 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-110A complies with GlobalPlatform® Card Specifications v2.2 (depending on UICC configuration) and related amendments.

4.2 Algorithms and cryptography

The ST4SIM-110A 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-110A also supports the "3GPP test algorithm" for test profiles.

In order to increase security performance, the ST4SIM-110A 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-110A provides a cryptographic co-processor with asymmetric cryptography capabilities.

For applications requiring the strongest level of cryptography, the ST4SIM-110A 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-110A 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 ST33G1M2A to guarantee the best security level (for more information, contact the local STMicroelectronics sales office).

4.3 Over the air (OTA) functionality

The ST4SIM-110A 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-110A . In addition, the ST4SIM-110A integrates a DNS mechanism allowing the card to request the HTTPS server address from a DNS server.

The ST4SIM-110A 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-110A 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-110A 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.

4.4 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-110A 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.

Volatile memory management is based on an STMicroelectronics patented mechanism that optimizes the available resources for the enabled profile while guaranteeing resources for the downloading profile and the disabled profiles.

5 Electrical characteristics

This section summarizes the operating and measurement conditions, and the DC and AC characteristics of the device. The parameters in the DC and AC characteristic tables that follow are derived from tests performed under the measurement conditions summarized in the relevant tables. Users should check that the operating conditions in their circuit match the measurement conditions when relying on the quoted parameters.

5.1 Absolute maximum ratings

Table 1. **Absolute maximum ratings**

Symbol	Parameter	Value	Unit
V_{CC}	Supply voltage	–0.3 to 6.5	V
V_{IO}	Input or output voltage relative to ground	–0.3 to V_{CC} +0.3	V
T_A	Ambient operating temperature	–40 to +105	°C
T_{STG}	Storage temperature (Please refer to package specification)	–65 to +150	°C
T_{LEAD}	Lead temperature during soldering	See (1)	°C
V_{ESD}	Electrostatic discharge voltage according to JESD22-A114, Human Body Model	4000	V

1. *Compliant with JEDEC standard J-STD-020D (for small-body, Sn-Pb or Pb-free assembly), the ST ECOPACK® 7191395 specification, and the European directive on Restrictions on Hazardous Substances (RoHS directive 2011/65/EU of July 2011).*

Note: *Stresses listed above may cause permanent damage to the device. This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operational sections of the specification is not implied.*

Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

5.2 Recommended power supply filtering

As mentioned in Section 6.1.2 Pinout information, the power supply of the circuit must be filtered using the circuit shown in the following figure.

Figure 3. **Recommended filtering capacitors on V_{CC}**

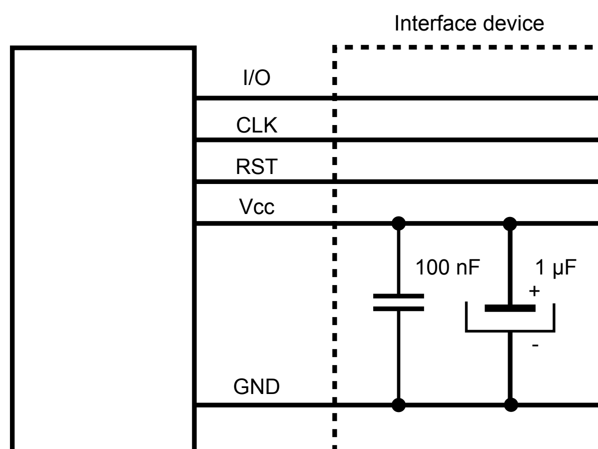


Table 2. **Maximum V_{CC} rising slope**

Symbol	Parameter	Value	Unit
S_{VCC}	Maximum V_{CC} rising slope	5	V / µs

5.3 AC and DC characteristics

These characteristics are compliant with ETSI TS 102 671 release 12.

6 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.

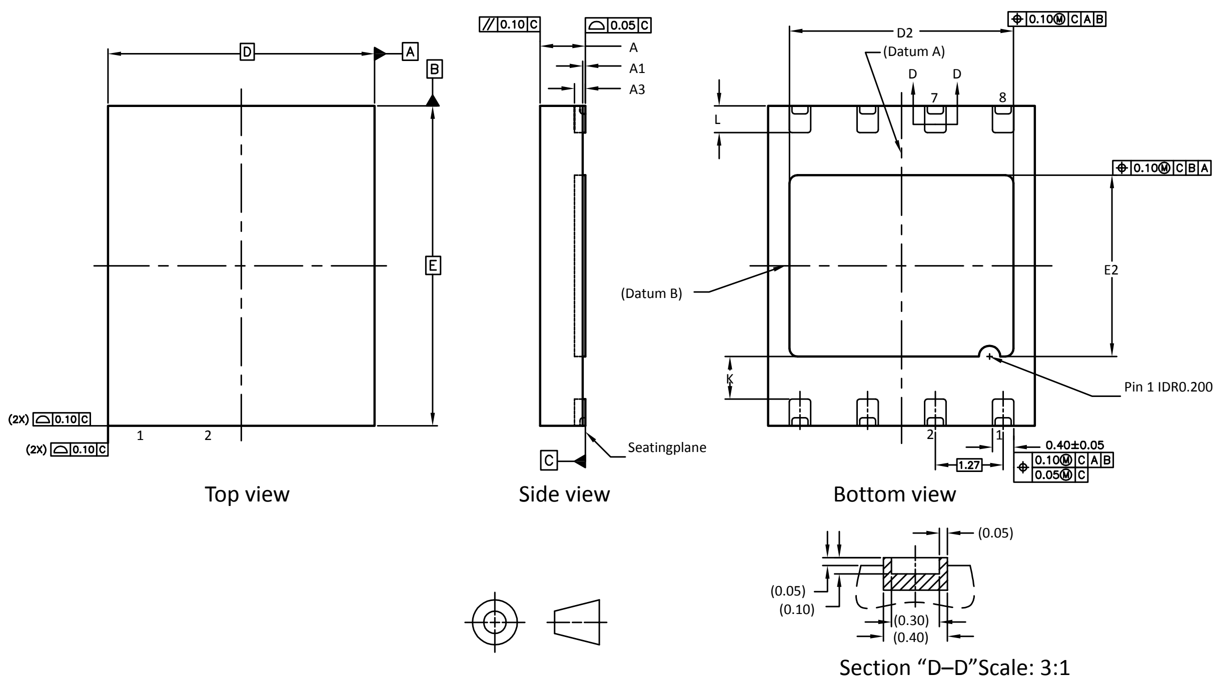
6.1 VFDFPN8 package information

VFDFPN8 is a "very thin fine pitch dual flat no lead package" with wettable flanks, dimensions 5 × 6 mm and 1.27 mm pitch.

This package is Automotive grade and compliant with JEDEC J-STD-020D (MSL1 specification).

It is also compliant with MFF2 (Machine-to-machine form factor 2) ETSI specifications (M2M UICC - TS102.671).

Figure 4. **VFDFPN8 - outline**



Note: Drawing is not to scale.

Table 3. **VFDFPN8 - mechanical data**

Symbol	Millimeters			Inches (1)		
	Min	Typ	Max	Min	Typ	Max
A	0.700	0.850	1.000	0.0276	0.0335	0.0393
A1	0	0.020	0.050	0	0.0008	0.0012
A3	-	0.200	-	-	0.0079	-
b	0.350	0.400	0.480	0.0138	0.0157	0.0189
D	-	5.000	-	-	0.1969	-
E	-	6.000	-	-	0.2362	-
e	-	1.270	-	-	0.0500	-
L	0.400	0.500	0.600	0.0157	0.0197	0.0236
D2	4.100	4.200	4.300	0.1614	0.1654	0.1693
E2	3.300	3.400	3.500	0.1299	0.1339	0.1378

1. *The dimensions are converted from mm and rounded to 4 decimal digits.*

6.1.1 Wettable flank for manufacture of inspectable solder joint

Traditional lead free packages tend be critical components in high reliability application, due to inspection issues of the solder joint between the leads and the PCB pads.

Figure 5. **Regular DFN (non-wettable flank)**

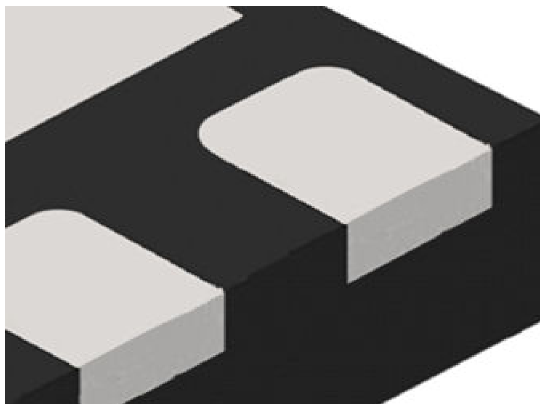
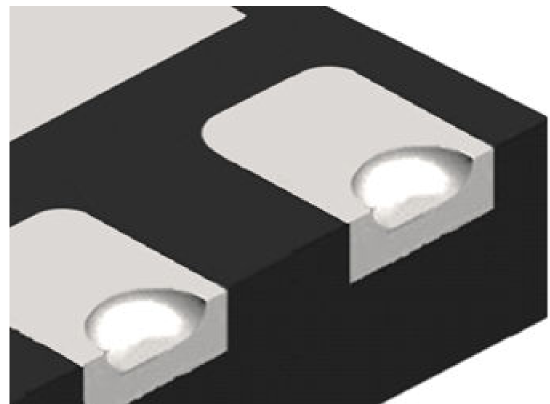


Figure 6. **DFN wettable flank**



VFDFPN8 package is constructed with "WETTABLE" flanks, a "dimpled" pad formed during the half-etching step of the lead frame manufacturing process.

The wettable flank feature, in conjunction with an optimized board mount process, promotes formation of solder joints which can be easily inspected. The presence of a solder fillet improves the inspection capability of the solder joints by automated optical inspection.

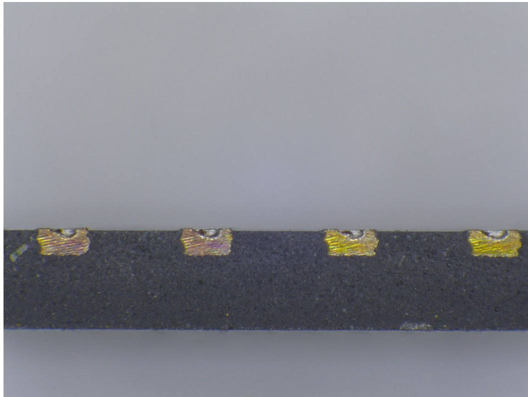


Figure 7. Solder joint side view

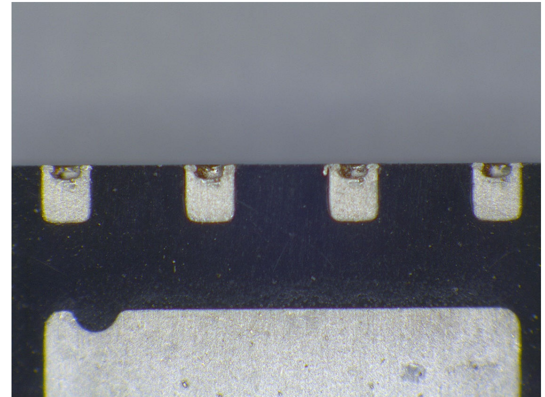


Figure 8. Solder joint top view

This package is compliant with machine to machine form factor defined by ETSI in TS 102 671.

6.1.2 Pinout information

This package is compatible with the MFF2 package defined by ETSI 102 671 release 12. The pinout details are described in the following figure and table together with PCB integrations recommendations in Figure 10.

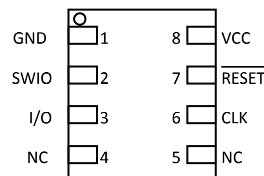
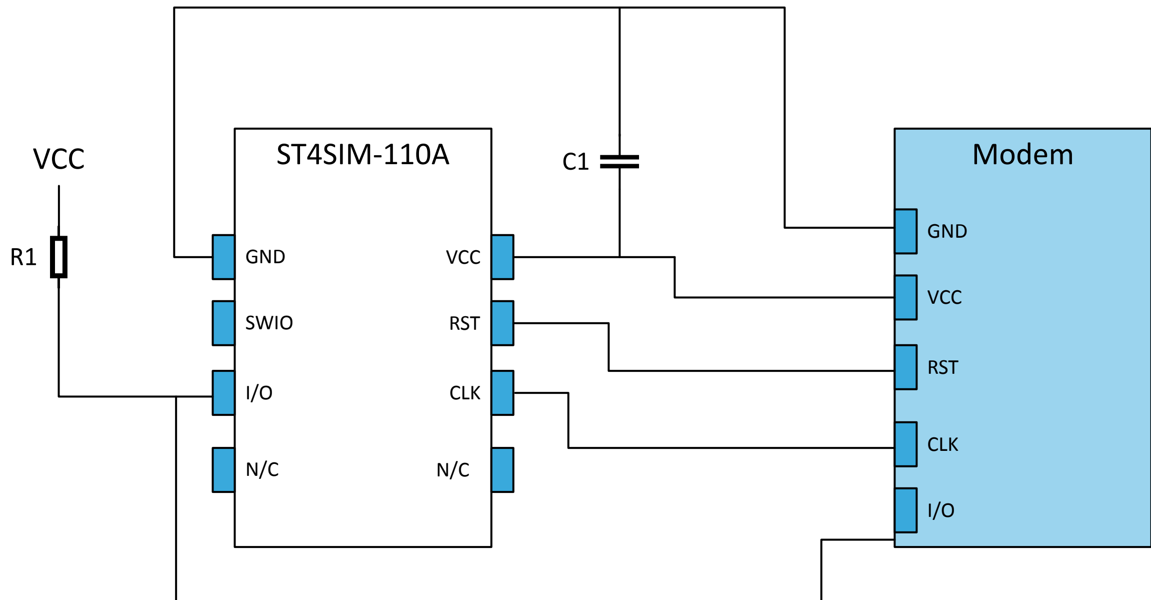


Figure 9. VFDFPN8 pinout (top view)

Table 4. Pin descriptions

Name	Description	Pin state
GND	Ground supply	-
SWIO	Not used	Input pull-up
$\overline{\text{RESET}}$	External reset	Input pull-down
I/O	Input/output	Pull-down then pull-up after card activation
CLK	External clock	Pull-down
VCC	Power supply	-
NC	Not connected internally	-

Figure 10. **ST4SIM-110A PCB integration recommendations**



Note: C1 decoupling capacitors as recommended in Figure 3. Recommended filtering capacitors on VCC.
R1: 20 kΩ external pull-up recommended on I/O.

6.1.3 Tape and reel packing

Surface-mount packages is available in tape and reel packing . The reels have a 13" nominal diameter and contain 4000 devices each.

Reels are in, either antistatic or conductive, plastic with a black conductive cavity tape. The cover tape is transparent antistatic or conductive.

The devices are positioned in the cavities with the identifying pin (normally Pin “1”) on the same side as the sprocket holes in the tape.

The STMicroelectronics Tape & Reel specifications are compliant to the EIA 481-A standard specification.

Table 5. **Packing on tape and reel**

Package	Description	Tape width	Tape pitch	Reel diameter	Quantity per reel
VFDFPN8 5 x 6	Flat package, no lead 5 x 6 mm.	12 mm	8 mm	13 in.	4000

Figure 11. 13 " reel diagram

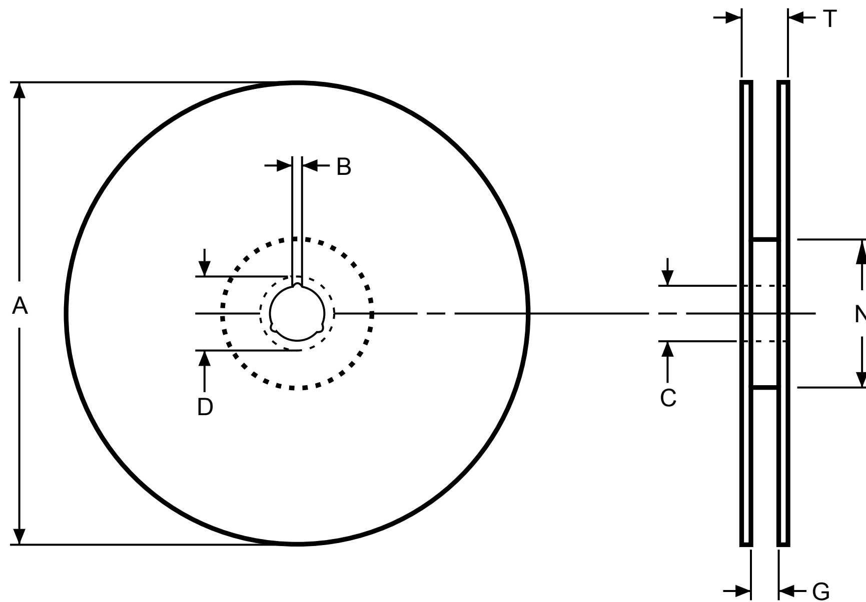


Table 6. 13" reel dimensions

Reel size	Tape size	A max	B min	C	D min	G max	N min	T max	Unit
13”	12 mm	330	1,5	13 ±0.25	20.2	12.6	100	18.4	mm

Figure 12. Leader and trailer

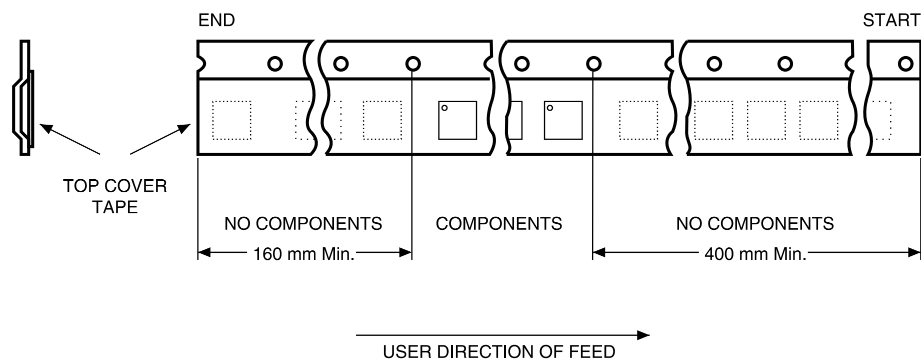
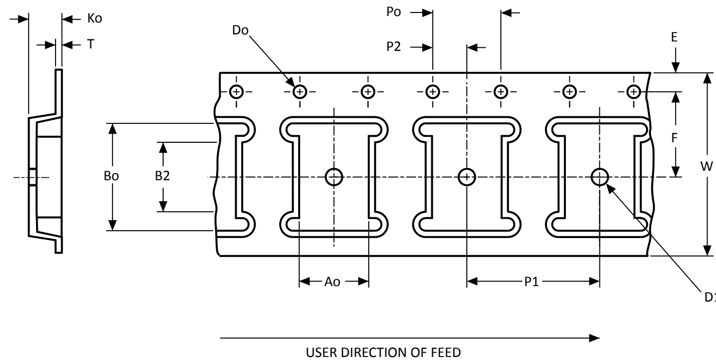
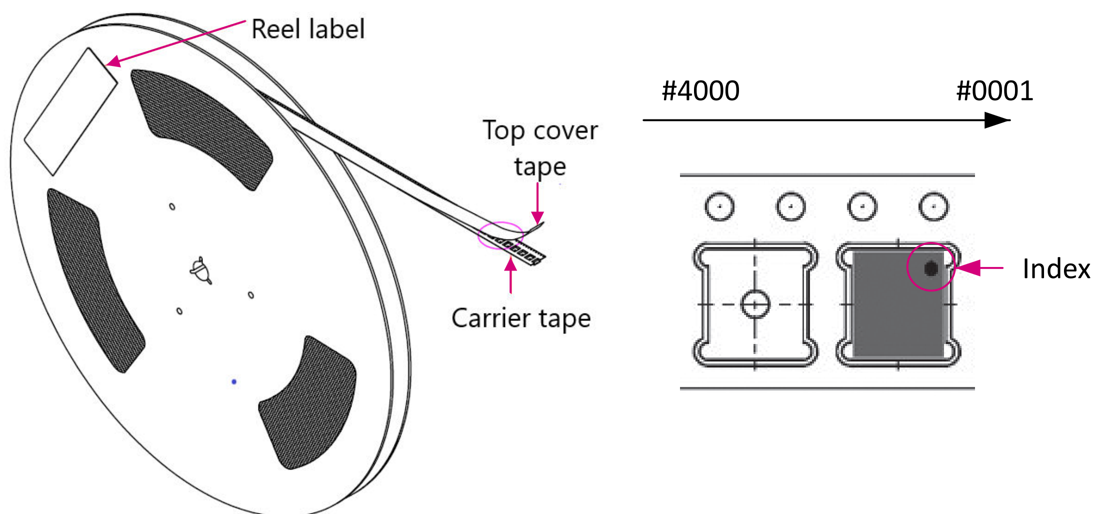


Figure 13. Embossed carrier tape for VFDFPN8 (5 × 6 mm)



Note:
1. *Cumulative tolerance of 10 sprocket hole pitch = ±0.20 mm.*
2. *Pocket position relative to sprocket hole is measured as the true position of the pocket, not the pocket hole.*
3. *A0 and B0 are calculated on a plane at a distance "R" above the bottom of the pocket.*
4. *Unless otherwise specified, all dimensions are in millimeters, and decimal values of the form x.x are with ±0.2 tolerance whereas values of the form x.xx are with ±0.10 tolerance.*
5. *Drawing is not to scale*

Figure 14. Component orientation



6.2 TSSOP20 package information

The TSSOP20 is a 20-lead thin shrink small-outline, 6.5 x 4.4 mm, 0.65 mm pitch, package.

For additional information on the TSSOP20 package pinout, contact the local STMicroelectronics sales office.

7 Acronyms

Table 7. 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
SMS	Simple message system
TAR	Toolkit application reference
TLS	Transport layer security
UICC	Universal integrated circuit card
UMTS	Universal mobile telecommunications systems

Revision history

Table 8. **Document revision history**

Date	Version	Changes
19-Dec-2019	1	Initial release.
19-Jan-2021	2	Updated: • Document title • Section Features • Section Applications • Section 1 Description Added: • Section 4 Card OS technical features • Section 4.1 Supported standards and networks • Section 5 Electrical characteristics • Section 6 Package information Removed • Supported standards and networks section • Algorithms and cryptography section

Contents

1 **Description** 3

2 **Cellular connectivity solutions overview** 4

3 **Additional embedded secure element (eSE)** 5

4 **Card OS technical features** 6

4.1 Supported standards and networks 6

4.2 **Algorithms and cryptography** 6

4.3 Over the air (OTA) functionality 6

4.4 Memory management 7

5 **Electrical characteristics** 8

5.1 Absolute maximum ratings 8

5.2 Recommended power supply filtering 8

5.3 AC and DC characteristics 9

6 **Package information** 10

6.1 VFDFPN8 package information 10

6.1.1 Wettable flank for manufacture of inspectable solder joint 11

6.1.2 Pinout information 12

6.1.3 Tape and reel packing 13

6.2 TSSOP20 package information 15

7 **Acronyms** 16

Revision history 18

List of tables

Table 1. Absolute maximum ratings . . . 8
Table 2. Maximum V_{CC} rising slope . . . 9
Table 3. VFDFPN8 - mechanical data . . . 11
Table 4. Pin descriptions . . . 12
Table 5. Packing on tape and reel . . . 13
Table 6. 13" reel dimensions . . . 14
Table 7. Glossary . . . 16
Table 8. Document revision history . . . 18

List of figures

Figure 1. SIM and eSIM architecture overview 4
Figure 2. ST4SIM-110A architecture eSIM & eSE overview 5
Figure 3. Recommended filtering capacitors on V_{CC} 8
Figure 4. VFDFPN8 - outline 10
Figure 5. Regular DFN (non-wettable flank) 11
Figure 6. DFN wettable flank 11
Figure 7. Solder joint side view 12
Figure 8. Solder joint top view 12
Figure 9. VFDFPN8 pinout (top view) 12
Figure 10. ST4SIM-110A PCB integration recommendations 13
Figure 11. 13 " reel diagram 14
Figure 12. Leader and trailer 14
Figure 13. Embossed carrier tape for VFDFPN8 (5 × 6 mm) 15
Figure 14. Component orientation 15

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST's terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers' products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to www.st.com/trademarks. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.

© 2021 STMicroelectronics – All rights reserved