

eSIM GSMA 5G system-on-chip solution for 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-201S](#)

Features

- Remote SIM provisioning compliant with GSMA M2M and TCA specifications
- Bootstrap connectivity profile provided by a trusted partner
- Multiple connectivity profiles hosted
- Compliant with 3G / 4G (LTE) / 5G / NB-IoT / CAT-M networks
- Network access applications supported: SIM / USIM / ISIM / CSIM
- Secure element access control (ARF / PKCS#15)
- Support of test profiles with local switch

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)
- WLCSP11

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

- GSMA SGP.02 v4.2
- TCA interoperable profile v2.3.1.
- Java® Card v3.0.5 classic
- GlobalPlatform® card specification v2.3, including GP amendments A, B, C, D and E
- ETSI, 3GPP and 3GPP2 release 16
- Power saving features (PSM and eDRX) defined by ETSI

Certification

- GlobalPlatform®-certified "ST4SIM-201 V1"
- GSMA eSA certified

Applications

- Cellular Connected Nodes
- LTE, 5G, LPWA (LTE-M, NB-IoT)
- Asset tracking
- Smart metering (Gas, Water, Electricity)
- Connected healthcare devices

1 Description

The **ST4SIM-201S** is an STMicroelectronics top-class GSMA embedded SIM (eSIM or eUICC) product designed for all IoT devices.

It is compliant with the GSM Association (GSMA) remote provisioning specification SGP.02 v4.2.

The device can remotely manage different MNO profiles while ensuring the appropriate security level to all eUICC 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 v3.0.5 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. 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.

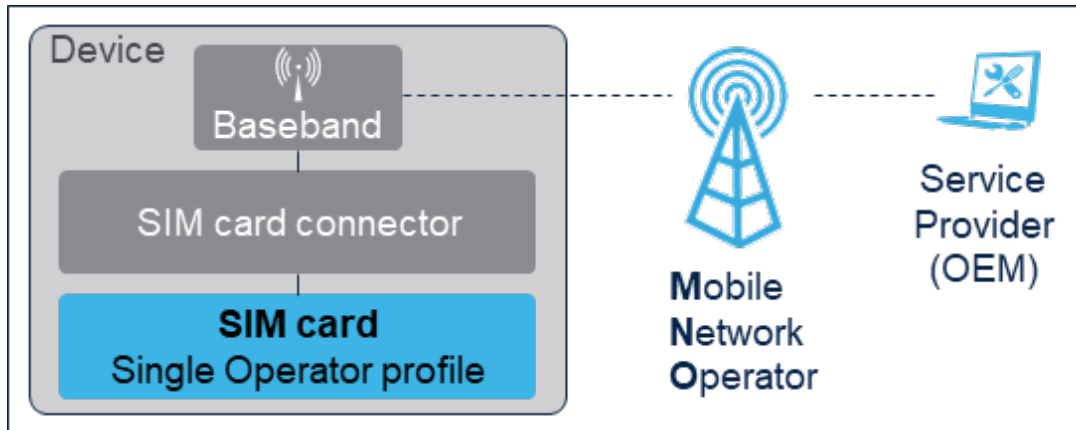


2 Cellular connectivity solutions overview

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.

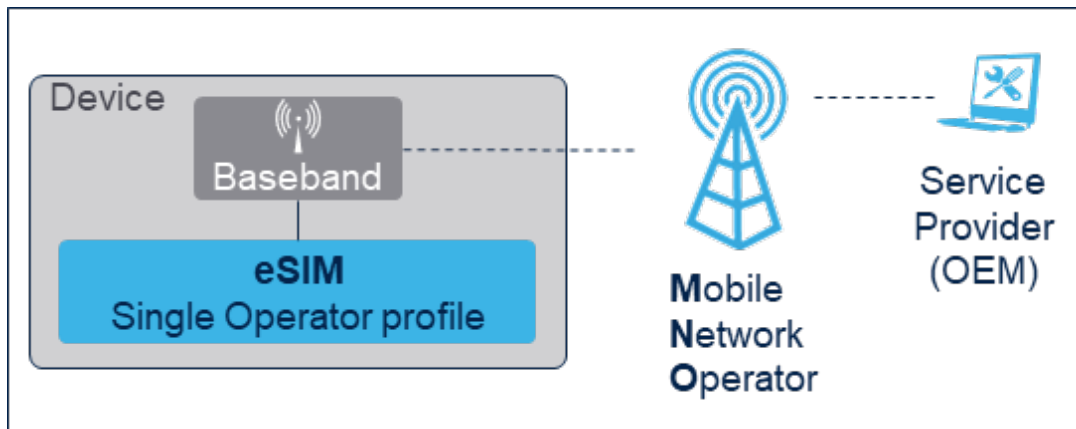
Moreover, a cellular solution is simple to deploy. This solution is mainly composed of the modem (baseband), the SIM card connector and the plastic SIM card. This is the traditional SIM concept inherited from the mobile phone.

Figure 1. SIM solution overview



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

Figure 2. eSIM solution overview



These traditional solutions are simple but the SIM / eSIM only supports one cellular connectivity profile at a time for one network operator. In this case, if the operator needs to be changed, the SIM / eSIM solution must be changed.

The eSIM GSMA solution extends this traditional SIM / eSIM solution.

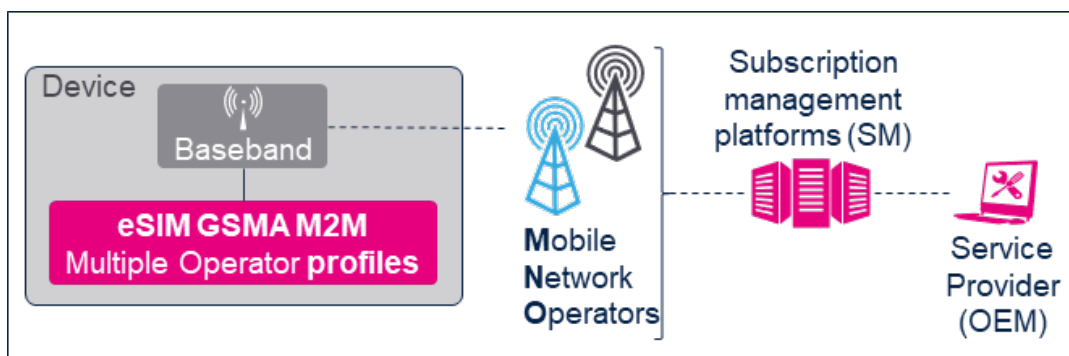
3 eSIM GSMA solution

The **ST4SIM-201S** is a GSMA eSIM solution compliant with the eSIM M2M specifications from the GSM Association (GSMA). This solution integrates a new secure architecture and complete ecosystem able to manage cellular network connectivity remotely without impacting the eSIM component.

Thanks to this eSIM technology, IoT devices can now be deployed to the field with one network connectivity solution and if at some later stage, this solution needs to be changed, a new one can be put in place through the network. So, no need for a product recall, nor product maintenance.

This solution is flexible and does not depend on a particular operator. For M2M, including industrial and automotive markets, this solution is service-oriented; the profile is remotely controlled by the service provider through a platform (push model). In this case, end-user interaction is not required.

Figure 3. eSIM GSMA solution overview

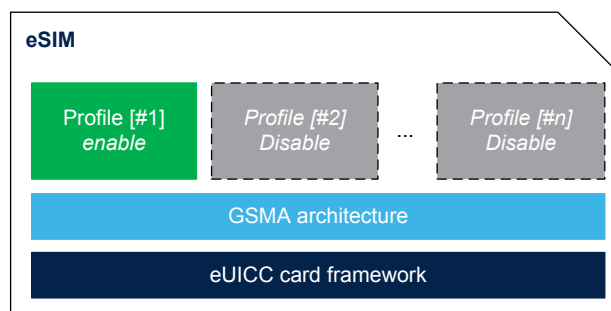


The **ST4SIM-201S** is interoperable with large subscription management platforms already deployed in the field. STMicroelectronics has attended all test sessions driven by GlobalPlatform (including PoC on SM-SR changes initiated by GSMA) and submitted all the platform solution interfaces (ES5, ES6 and ES8 interfaces). The device offers a complete ecosystem thanks to STMicroelectronics trusted partners. Our partners provide the connectivity profile and the subscription management platform to provision and remotely manage operator profiles. (Contact the local STMicroelectronics sales office for more details on STMicroelectronics trusted partners)

Based on a certified Common Criteria EAL5+ secure hardware solution, the **ST4SIM-201S** is a GSMA eSA certified solution compliant with the GSMA eUICC M2M specification SGP.02 v4.2. It provides a flexible and scalable solution while maintaining the best level of security.

The **ST4SIM-201S** integrates the GSMA architecture with the profile management mechanisms. A profile contains the operator network data related to a subscription (operator's credentials, file system, PINs/PUKs, network authentication, application and so on). Each profile is independent of other profiles.

Figure 4. eSIM architecture overview



This profile is described by the TCA interoperable profile package specification.

The **ST4SIM-201S** fully supports TCA interoperable profile package v2.3.1. No proprietary features are introduced and profiles are coded according to ASN.1 / DER coding.

The device fully supports TCA interoperable profile package v2.3.1. No proprietary features are introduced and profiles are coded according to ASN.1 / DER coding.

The device is an interoperable solution. The device already integrates most of main operators (MNO / MVNO) and it is possible to integrate any operator profile or personalized profile compliant with the TCA specification.

4 Card OS technical features

4.1 Supported standards and networks

The **ST4SIM-201S** solution complies with the standard networks (3G / 4G (LTE) / 5G) and low power networks (NB-IoT / CAT-M).

From a technical point of view, the **ST4SIM-201S** 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-201S** complies with GlobalPlatform® card specification v2.3 (depending on UICC configuration) and related amendments.

4.2 Algorithms and cryptography

The **ST4SIM-201S** supports the following standard authentication algorithms:

- CAVE
- MILENAGE
- TUAK

The MILENAGE algorithm enables authorized access to UMTS/LTE/5G 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-201S** also supports the "3GPP test algorithm" for test profiles.

In order to increase security performance, the **ST4SIM-201S** 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-201S** provides a cryptographic co-processor with asymmetric cryptography capabilities.

For applications requiring the strongest level of cryptography, the **ST4SIM-201S** 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-201S** 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).

4.3 Over the air (OTA) functionality

The **ST4SIM-201S** 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-201S**. In addition, the **ST4SIM-201S** integrates a DNS mechanism allowing the card to request the HTTPS server address from a DNS server.

The **ST4SIM-201S** 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-201S** 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-201S** 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 5G 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-201S** 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

The power supply of the circuit must be filtered using the circuit shown in the following figure.

Figure 5. Recommended filtering capacitors on V_{CC}

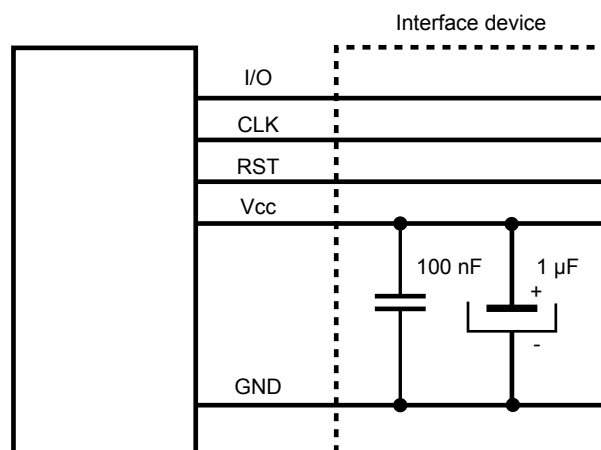


Table 2. Maximum V_{CC} rising slope

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.

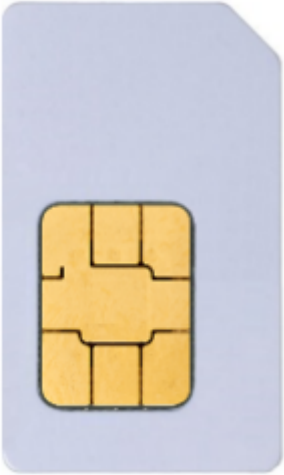

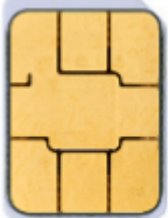
6.1 2FF, 3FF or 4FF plugin card package information (based on D18 micromodule)

The **ST4SIM-201S** card is based on flexible plastic chip cards, composed of ABS and Polycarbonate, improving all round resistance in an industrial environment. This card contains a STMicroelectronics industrial grade D18 micromodule.

All elements; card and micromodule, are designed to run at a temperature of -40 °C to +105 °C.

The **ST4SIM-201S** is available for different card plugin packages as detailed in the table below.

Table 3. SIM plugin package types and dimensions

Package	Mini SIM (2FF)	Micro SIM (3FF)	Nano SIM (4FF)
Package format			
Height	25 mm (±0.1 mm)	15 mm (±0.1 mm)	12.3 mm (±0.1 mm)
Width	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)	0.67 mm (+ 0.03 mm / - 0.07 mm)

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

6.1.1 D18 micromodule pinout information

The contact of D18 micromodule are compliant with ISO/IEC 7816-3 standard. The contact assignment layout is given in the figure below and contact description is in the following table.

Figure 6. D18 micromodule contact assignment

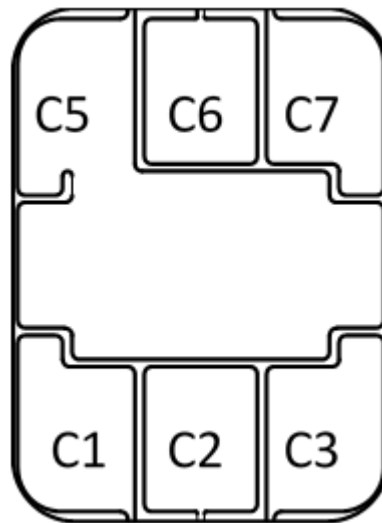


Table 4. D18 contact descriptions

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

6.2 WLCSP11 package information

For information on the wafer level chip scale package (WLCSP11) pinout, contact the local STMicroelectronics sales office.

7 Acronyms and abbreviations

Table 5. Acronyms and abbreviations

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
GSMA	The GSM Association
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
OEM	Original equipment manufacturer
OTA	Over the air

Term	Description
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
WLCSP	Wafer level chip size package

Revision history

Table 6. Document revision history

Date	Version	Changes
23-May-2022	1	Initial release.

Contents

1	Description	3
2	Cellular connectivity solutions overview	4
3	eSIM GSMA solution	5
4	Card OS technical features	7
4.1	Supported standards and networks	7
4.2	Algorithms and cryptography	7
4.3	Over the air (OTA) functionality	7
4.4	Memory management	8
5	Electrical characteristics	9
5.1	Absolute maximum ratings	9
5.2	Recommended power supply filtering	9
5.3	AC and DC characteristics	10
6	Package information	11
6.1	2FF, 3FF or 4FF plugin card package information (based on D18 micromodule)	11
6.1.1	D18 micromodule pinout information	11
6.2	WLCSP11 package information	12
7	Acronyms and abbreviations	13
	Revision history	15

List of tables

Table 1.	Absolute maximum ratings	9
Table 2.	Maximum V_{CC} rising slope	9
Table 3.	SIM plugin package types and dimensions	11
Table 4.	D18 contact descriptions	12
Table 5.	Acronyms and abbreviations	13
Table 6.	Document revision history	15

List of figures

Figure 1.	SIM solution overview	4
Figure 2.	eSIM solution overview	4
Figure 3.	eSIM GSMA solution overview	5
Figure 4.	eSIM architecture overview	5
Figure 5.	Recommended filtering capacitors on V_{CC}	9
Figure 6.	D18 micromodule contact assignment	12

IMPORTANT NOTICE – 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 acknowledgment.

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, 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.

© 2022 STMicroelectronics – All rights reserved