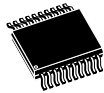


eSIM system-on-chip solution for automotive applications



VFDFPN8

5 × 6 mm,

Wettable flanks
(MFF2)

TSSOP20

6.5 × 4.4 mm

Features



- AEC-Q100 qualified Grade 2
- Remote SIM provisioning compliant with GSMA M2M and SIMalliance specifications
- Bootstrap connectivity profile
- Up to 7 profiles (depending on memory size)
- 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 ST33G1M2A0
- 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 Grade 2)
- Operating temperature: -40°C to +105°C
- Common Criteria EAL5+

[Product status link](#)[ST4SIM-200A](#)

ECOPACK-compliant packages

- DFN8 Wettable Flank (MFF2)
- TSSOP20

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 brainpoolP256r1
- Authentication algorithm: MILENAGE, TUAK, CAVE

Software standard compliancy

- GSMA SGP.02 v3.2
- SIMalliance interoperable profile v2.1
- 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 your local STMicroelectronics sales office)
- Power saving features (PSM and eDRX) defined by ETSI release 13

Certification

- GlobalPlatform-certified "Muse eUICC-i2 v1" compliant with GSMA SGP.02 v3.2

Applications

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

1 Description

The **ST4SIM-200A** is an STMicroelectronics top-class embedded SIM (eSIM or eUICC) product designed for the automotive ecosystem.

This solution is based on the ST33G1M2A0, an automotive grade hardware solution, AEC-Q100 qualified grade 2.

The **ST4SIM-200A** is compliant with the GSM Association (GSMA) remote provisioning specification SGP.02 v3.2. It can remotely manage profiles of different MNOs while ensuring the appropriate security level to all eUICC stakeholders (user, MNO, OEM, hardware integrator, service provider, and so on).

The **ST4SIM-200A** can include an embedded secure element to store credential and/or independent applications directly managed by the MCU (or by another OEM element).

The **ST4SIM-200A** provides a secure and interoperable Java Card environment compliant with Java Card v3.0.4 classic. Moreover, the **ST4SIM-200A** integrates the most advanced UICC features compliant with GlobalPlatform, ETSI, 3GPP, 3GPP2 specifications.

The **ST4SIM-200A** integrates a dynamic memory management with Java Card garbage collection mechanism optimizing the usage of the memory.

The **ST4SIM-200A** 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.

arm



2 Supported standards and networks

The [ST4SIM-200A](#) 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-200A](#) is compliant with GlobalPlatform Card Specifications v2.2 (depending on UICC configuration) and related amendments.

3 Remote SIM provisioning

The remote SIM provisioning, defined by GSMA in SGP.02 v3.2 specification for M2M, extends the traditional SIM and offers a scalable solution while maintaining the best level of security.

The “traditional SIM card” is usually owned and issued by one network operator. With this solution, the end user must physically change the SIM card to change the operator or subscription. In most embedded solutions, this solution is not satisfactory.

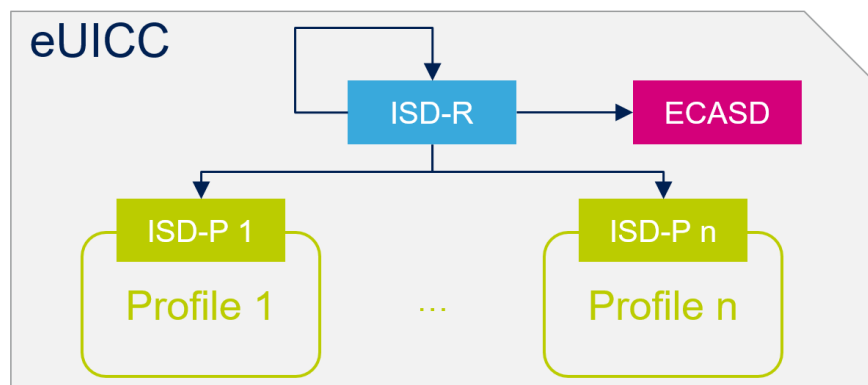
The **ST4SIM-200A**, using the remote SIM provisioning, provides an embedded SIM solution (called an eSIM or eUICC) which is flexible and independent of operator. It is now possible to change the profile without changing physically the eSIM.

A profile contains the operator network data related to a subscription, including the operator’s credentials (file system, PINs/PUKs, NAA authentication information) and applications. Each profile is independent of the other profiles. In this way, it is possible to have in two profiles an application with the same AID, TAR or global service.

This profile is described by SIMalliance interoperable profile package specification.

The **ST4SIM-200A** architecture is compliant with GSMA SCP.02 v3.2 specifications and supports all mechanisms performing profile management.

Figure 1. Security domain architecture overview



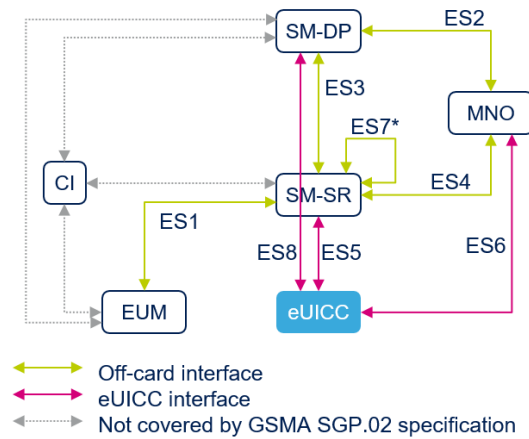
The **ST4SIM-200A** can host up to 7 profiles. Each profile has the memory size available in the **ST4SIM-200A** or can have a specific memory size coded using the cumulative granted memory defined by GlobalPlatform amendment C.

The **ST4SIM-200A** fully supports SIMalliance interoperable profile package v2.1. No proprietary features are introduced and profiles are coded according to ASN.1 / DER coding.

The **ST4SIM-200A** is an interoperable solution. The **ST4SIM-200A** already integrates most of main operators (MNO / MVNO) and it is possible to integrate any operator’s profile or personalized profile compliant with the SIMalliance specification. STMicroelectronics also has several trusted partners providing connectivity for bootstrap profile (contact your local STMicroelectronics sales office).

For machine-to-machine, 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, the user interaction is not required.

Figure 2. eUICC Remote provisioning system



* Interface between two SM-SR entities for the change of SM-SR

The **ST4SIM-200A** supports all interfaces described by GSMA SGP.02:

- ES5 interface (SM-SR/eUICC),
- ES8 interface (SM-DP/eUICC),
- ES6 interface (MNO/ eUICC).

The eSIM protocols provide security and integrity for data transfer: with the **ST4SIM-200A**, the profile can be downloaded by using SCP03t over HTTPS. Profile download over CAT-TP is not supported.

The **ST4SIM-200A** is also interoperable with large subscription management platforms already deployed on the field. STMicroelectronics has attended all Test Fest sessions driven by GlobalPlatform and PoC on SM-SR changes initiated by GSMA.

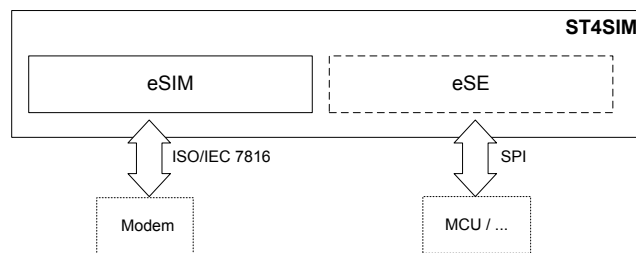
In addition, STMicroelectronics has several trusted partners providing platform services to provision and remotely manage operator profiles (Contact your local STMicroelectronics sales office).

4 Additional embedded secure element (eSE)

The **ST4SIM-200A** is a solution combining an eSIM with an embedded secure element (eSE) section inside the same chip.

This eSE section can be used to provide secure storage, cryptographic services, etc. via Java card applets.

Figure 3. ST4SIM-200A 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 WLCSP packages including ISO and SPI protocols.

The embedded secure element is optional and configurable.

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

5 Algorithms and cryptography

The [ST4SIM-200A](#) 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-200A](#) also supports the "3GPP test algorithm" for test profiles.

In order to increase security performance, the [ST4SIM-200A](#) also incorporates a ratification counter that limits the number of authentication attempts to prevent brute-force attacks from breaking algorithms. In addition, all algorithms support dedicated countermeasures for DPA/SPA attacks.

Besides standard symmetric cryptography and hashing algorithms (DES, Triple DES, AES, MD5, ...), the [ST4SIM-200A](#) provides a cryptographic co-processor with asymmetric cryptography capabilities.

For applications demanding the strongest level of cryptography, the [ST4SIM-200A](#) 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-200A](#) 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 respects the chip security guidelines of the ST33G1M2A0 to guarantee the best security level (for more information, contact your local STMicroelectronics sales office).

6 Over the air (OTA) functionality

The [ST4SIM-200A](#) 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 Global Platform v2.2 and the related amendment B (allowing the possibility to perform remote applet management and remote file management over HTTP/TLS).

TLS v1.0, 1.1 and 1.2 are available in the [ST4SIM-200A](#). In addition, the [ST4SIM-200A](#) integrates a DNS mechanism allowing the card to request the HTTPS server address from a DNS server.

The [ST4SIM-200A](#) makes it possible to remotely control over the air the execution of APDU commands to administrate the card contents. It also allows proactive commands to interact with the host device.

The [ST4SIM-200A](#) 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-200A](#) 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.

7 Memory management

The OTA mechanism is completed by 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/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-200A** is capable of enhancing intrinsic Flash memory cells for files requiring intense update and higher 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.

8 Acronyms

Table 1. List of acronyms

| Acronym | Description |
|---------|---|
| 3GPP | 3rd generation partnership project |
| AEC | Automotive electronics council |
| 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 subsystem |
| IoT | Internet of things |
| ISIM | IP multimedia services identity module |
| ISO | International organization for standardization |
| JEDEC | Semiconductor engineering standardization (Joint electron device engineering council) |
| LTE | Long-term evolution (telecommunication) |
| MD5 | Message-digest algorithm producing a 128-bit hash value |
| M2M | Machine-to-machine |
| MNO | Mobile network operator |
| MNO-SD | Mobile network operator security domain |
| MVNO | Mobile virtual network operator |
| NAA | Network access application |
| NB-IoT | NarrowBand-Internet of Things |
| NIST | National Institute of Standards and Technology |

| Acronym | Description |
|---------|--|
| OEM | Original equipment manufacturer |
| OTA | Over the air |
| PIN | Personal identification number |
| PKCS | Public key cryptographic standards |
| PoC | Proof of concept |
| PSM | Power saving mode |
| PUK | PIN unlock key |
| RAM | Remote application management |
| RFM | Remote file management |
| RISC | Reduced instruction set computer |
| RSA | Public-key cryptosystem (Ron Rivest, Adi Shamir and Leonard Adleman) |
| SCP | Secure channel protocol |
| SIM | Subscriber identity module |
| SM-DP | Subscription manager - Data preparation |
| SMS | Short message service |
| SM-SR | Subscription manager - Secure routing |
| UICC | Universal integrated circuit card |
| UMTS | Universal mobile telecommunications system |
| USIM | Universal subscriber identity module |
| SE | Secure element |
| TAR | Toolkit application reference |
| TLS | Transport layer security |
| WLCSP | Wafer level chip size package |

Revision history

Table 2. Document revision history

| Date | Version | Changes |
|-------------|---------|------------------|
| 19-Dec-2019 | 1 | Initial release. |

Contents

| | | |
|----------|---|-----------|
| 1 | Description | 3 |
| 2 | Supported standards and networks | 4 |
| 3 | Remote SIM provisioning | 5 |
| 4 | Additional embedded secure element (eSE) | 7 |
| 5 | Algorithms and cryptography | 8 |
| 6 | Over the air (OTA) functionality | 9 |
| 7 | Memory management | 10 |
| 8 | Acronyms | 11 |
| | Revision history | 13 |
| | Contents | 14 |
| | List of tables | 15 |
| | List of figures | 16 |

List of tables

| | | |
|-----------------|-------------------------------------|----|
| Table 1. | List of acronyms | 11 |
| Table 2. | Document revision history | 13 |

List of figures

| | | |
|------------------|--|---|
| Figure 1. | Security domain architecture overview | 5 |
| Figure 2. | eUICC Remote provisioning system | 6 |
| Figure 3. | ST4SIM-200A architecture eSIM & eSE overview | 7 |

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.

© 2019 STMicroelectronics – All rights reserved