Connected security for IoT

Kenneth Huang
Marketing Manager
STMicroelectronics
# Connected security portfolio

**Worldwide sales & marketing offices**

**Manufacturing and personalization sites across the globe**

## EEPROM

<table>
<thead>
<tr>
<th>36%</th>
<th>Market share in 2022*</th>
</tr>
</thead>
<tbody>
<tr>
<td>20+</td>
<td>Billion units shipped to date</td>
</tr>
<tr>
<td>32Mbits</td>
<td>Smart Page EEPROM inventor</td>
</tr>
</tbody>
</table>

* Based on actual 3Q’22 Omdia Nov’22

## NFC Tags & Readers

<table>
<thead>
<tr>
<th>20%</th>
<th>Market share in 2022**</th>
</tr>
</thead>
<tbody>
<tr>
<td>34+</td>
<td>NFC Forum certified products</td>
</tr>
<tr>
<td>60+</td>
<td>Ecosystem: demos, boards and software package</td>
</tr>
</tbody>
</table>

** Based on ST internal analysis Feb’23

## Secure MCUs

<table>
<thead>
<tr>
<th>20%</th>
<th>Market share in 2022***</th>
</tr>
</thead>
<tbody>
<tr>
<td>15+</td>
<td>Billion units shipped to date</td>
</tr>
<tr>
<td>30+</td>
<td>Years of experience in security</td>
</tr>
</tbody>
</table>

*** Based on WSTS Feb’23

---

*ST* augmented
Page EEPROM ID card

Page EEPROM

- 8 to 32 Mbits with ECC
- Write: 2.3 ms
- Program: 1.2 ms
- Page erase: 1.1 ms
- Block erase: 4 ms
- Quad SPI output
- 500K cycles at full T
- 100 years retention

Ultra-low power operation

- 1.6 to 3.6 V
- SPI 80Mhz
- -40 to 85°C
- -40 to 105°C

SPI interface

- Wide voltage & temperature range
- Fast wake-up
- SPI single input
- SPI single/dual/quad output

Ultra low power

- Lowest operating current on market
- Peak current control
- Deep power down

Memory architecture

- Page size 512 bytes
- Write byte flexibility
- Fast program page
- Fast erase page, sector, block, chip
- Buffer load while program

High quality

- Error Code Correction (ECC)
- Safety flags
- Read only protection
- High endurance and retention

1.6 to 3.6 V
SPI 80Mhz
-40 to 85°C
-40 to 105°C

Ultra low power operation

SO8
DFN8
WLCSP
Bare die
## EEPROM specifications
### SPI interface & power consumption

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voltage range</td>
<td>1.6 to 3.6V</td>
</tr>
<tr>
<td>Temperature range</td>
<td>-40 to +85°C and 105°C</td>
</tr>
<tr>
<td>Wake up latency</td>
<td>30 µs</td>
</tr>
<tr>
<td>SPI interface</td>
<td>80 MHz SPI single/dual/quad output</td>
</tr>
<tr>
<td>Standby current</td>
<td>15 µA</td>
</tr>
<tr>
<td>Deep power down</td>
<td>0.6 µA</td>
</tr>
<tr>
<td>Read current</td>
<td>&lt; 500 µA</td>
</tr>
<tr>
<td>Erase current</td>
<td>&lt; 1mA</td>
</tr>
<tr>
<td>Program current</td>
<td>&lt; 2 mA</td>
</tr>
<tr>
<td>Write current</td>
<td>&lt; 1.5 mA</td>
</tr>
<tr>
<td>Peak current control</td>
<td>&lt; 3 mA</td>
</tr>
</tbody>
</table>

**Note:** typical values

### SPI interface

- Ultra low power

**Note:** typical values
- **Fast** page program: **512 bytes in 1.2ms**

- Buffer mode is **x1.75** faster than serial flash
  - Buffer mode hides SPI communication
  - Very efficient between 4MHz to 40Mhz

- To program 100k parts it takes:
  - ~ 33h with page EEPROM
  - ~ 55h with serial flash

**Save one production day!**
Page EEPROM – application benefits

Ultra-low power
- Very low operating consumption
- Current peak control

Manufacturing
- Program with buffer load
- Quad SPI 80Mhz Read

Boot code & FOTA
- Ultra fast erase time
- Fast program 512 bytes

Data logging & event recording
- High cycling endurance
- Fast byte write granularity

Safety guidelines
- Prog/erase status flag
- Read ECC flag
NFC non-smartphone products

Tags

STM32 microcontroller → ST25T
EEPROM

13.56MHz
NFC phone / RFID Reader

Industrial, Lighting, Consumer, Metering, Appliance, Healthcare, … (Fast Transfer Mode and SW upgrade) www.st.com/st25d

Dynamic tags

STM32 microcontroller → ST25D
EEPROM

13.56MHz
NFC phone / RFID Reader

POS & mPOS Terminals, Automotive, Access control, Gaming, … www.st.com/st25r

Readers

STM32 microcontroller → ST25R
RAM

13.56MHz
NFC phone

Consumer engagement, Asset tracking, Ticketing, Gaming, Brand protection, Access control, … www.st.com/st25t

or

Bank

or


ST25TV512C / 02KC ID card

Use cases
- Product Identification, asset tracking, consumer engagement, access control, gaming
- Tamper proof application, brand protection

Key Features
- ISO15693 and NFC Type V (long range operations, 26kb/s)
- Memory configuration: 512-bit and up to 2560-bit
- TruST25 Digital Signature (can be used into ANDEF: 2K-bit only)
- 24-bit Unique Tap Code (UTC) with anti-tearing
- Untraceable (by default possible) & Kill modes
- Tamper Detect pin for open / short detection
- Augmented NDEF: UID, UTC, Tamper status, custom field, PWD counter

Key Benefits
- Configurable User Memory Area
- Cloning Protection with Digital Signature (Cloud management)
- 60 years data retention, 100k cycles erase/write
ST25T temp protection tag
ST25DV-I2C-EVO
enhanced dynamic NFC Type 5 tag

Use cases
- Fast data exchange with NFC phones / HF readers
- Fast data transfer for MCU FW upgrade, fast data exchange
- Parameters settings and update, with in-the-box programming
- Data log download

Key features
- ISO15693 and NFC Type V
- Fast data transfer thanks to 256 Bytes buffer
- I2C write on 16-Byte page
- Low Power mode, < 1μA power consumption in Standby
- -40 to +125°C (I2C) industrial Grade 8 temperature range
- Energy harvesting function through RF
- I2C enhanced features (write time improved, address configurable, access priority…)

Key benefits
- Smart applications using a flexible interrupt GPO
- Enhanced protection with multiple 64-bit passwords
- Same 28.5pF internal RF tuning capacitor, as in ST25DV-I2C & M24LR
ST25D benefits all electronic devices

Simply more connected!

- Temperature sensor: STLM20
- Humidity sensor
- LAN/POL...
- WiFi / Zigbee/BT...
- LED Display
- MCU /BB/AP
- MEMs
- Light sensor
- GPS
- Dynamic NFC Tag
- LDOs
- Super cap
- NFC reader

- UID: Identification
- No on-board power is needed for R/W data → Good for PCB tracking
- Short read range: authorization, switch on / cut off control
- Easy to use: tape for BT / Wi-Fi pairing, data exchange

- In-factory programming
- App Launcher
- Power to system
- Device setup
- Wireless pairing
- Diagnostic
- SW upgrade
Improving user interface

ST25 solutions for devices without keypad or display: tag with I2C

Phone screen and App as user interface

Bidirectional data exchange From and to your device

Download data log or upload new settings

From your device cradle to grave
Thread commissioning over NFC

Use NFC to simplify the thread commissioning procedure by one tap

1. Read the device’s ID+commissioning credentials
2. Petitions to become a commissioner
3. Inform the OTBR that this device is going to request access to Thread Network
4. Send discovery requests on every Thread channel
5. The Joiner device receives a response from the OTBR
6. An encrypted session is started
7. The device is commissioned and ready to be used on Thread network
8. Start a SRP service to indicate its presence
9. Find the SRP service and gets the IPV6 address of the device
10. UDP messages can be exchanged to control the Thermostat
ST25 for IEEE 111073 PHD

IEEE 11073 PHD Profile
IEEE 11073-20601

Medical device dependent
Protocol

APDU ↔ NDEF
APDU ↔ FTM
NDEF R/W
FTM

BSP + Component driver

I2C

IEEE 11073-20601

APDU ↔ NDEF
APDU ↔ FTM
NDEF R/W
FTM

ST25 SDK

IEEE 11073 PHD Profile

ST25 SW

IEEE 11073 Stack

ST25 PHD SW Stack

Application layer

ST25 PHD FW

STM32

ST25DVxxKC

MCU

I2C

NFC

IEEE 11073-20601 PHD

ST25 PHD

NFC

iOS CoreNFC

Android NFC

iOS CoreNFC

Android NFC

NFC

FTM

APDU ↔ NDEF
APDU ↔ FTM
NDEF R/W
FTM

ST25 DVxxKC

I2C

AAPC

NFC

FTM

APDU ↔ NDEF
APDU ↔ FTM
NDEF R/W
FTM
Next gen UFD/SSD

ST25DV for lock / unlock management
### ST25D applications

<table>
<thead>
<tr>
<th>Batter user experience</th>
<th>Secure locked/unlocked</th>
<th>Energy harvesting</th>
<th>Parameter setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tape and download an app</td>
<td>Use an NFC phone to lock or unlock the private device with size and cost concern</td>
<td>Active E-paper panel/LED/low power device w/o on-board power</td>
<td>Data download / FW upgrade in production</td>
</tr>
<tr>
<td>Wireless pairing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data download/data -log</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NFC forum type 5 for long-range RF reading plus fast transfer improves time to market and user experience by tapping a phone**

- **Device needs to be powered**
- **Programming device needs to be plugged**

**Industrial, lighting, metering, consumer, appliance, healthcare, IoT…**

[www.st.com/st25d](http://www.st.com/st25d)
ST25R3916

high-performance NFC universal device & EMVCo reader

Use cases
• Ideal for Payment applications
• Access Control, Gaming, IOT and pairing

Key Features
• NFC Forum Universal Device (with CE mode)
• 1.6W output power at 5V with 2.5W peak current
• EMVCo 3.0 certification without external power amplifier
• Active Waveshaping, Noise Suppression Receiver
• Automatic Antenna Tuning
• -40°C to 105°C ambient temperature range (QFN)

Key Benefits
• Low power operation & Standby mode (capacitive wake-up)
• Works in challenging environment like noisy LCD displays
• Ideal for passing newest EMVCo standards
ST25R applications

ST25R3916 2.5W power for excellent interaction range and smallest antenna sizes, combined with advanced features for flexible design

Payment, access (Car, building…), gaming, consumables, authentication, interaction, data transfer…

Payment
- Contactless Payment

Car access
- Digital key for Door handle
- Start engine

Access control
- Smart lock
- Building / Hotel Access

Authentication
- Battery monitor for E-scooter
- Accessory management for printer, Air filter, medical test kit

www.st.com/st25r
What is our target?

Threats come when massive IoT devices connected

Major driver: IoT security awareness

STSAFE makes the node as a trusted device thanks to key and certificate provisioning service at ST trusted person center, allows the device to be authenticated automatically by the Clouds

+ more security features
  - Secure connection establishment
  - Secure storage
  - Secure FOTA

Mass market customers
Using STSAFE-A110 in the real world: cloud attachment & battery authentication

Cloud attachment

- The X.509 certificate stores in STSAFE-A in WiFi module providing a strict authentication of trusted IoT device from a specific Cloud account

- STSAFE-A with family certificate pre-attachment allows the device to be authenticated automatically by the Clouds (zero-touch)

See our blog to get more:
STSAFE-A110 and Secure Cloud Connectivity, a new way to automate device registration

Brand protection

- System running healthily is the key to protect its Brand
- The customer wants making sure genuine sub-boards connected to the system
- Stable power supply is key: STSAFE-A110 with certificate inside as a strong and trusted attestation, ensure the standard power supply modules are authenticated to deliver power
- No power will be delivered when unwanted/unstable power supply module connected to damage the system

STSAFE-A with provisioning service at certified ST facility: ensures secret keys & certificate personalized securely
Introducing the SIM concept

Subscriber Identity Module or Subscriber Identification Module

The SIM is
- Statically linked to a single operator
- Requires huge maintenance in case of operator swap
- Owned by operator
- Complex in term of logistic

- Based on a secure microcontroller hardware
- Stores all information identifying the subscriber and the telecom operator (MNO/MVNO)
- Provides to the modem all features to access the cellular network
- Is available in multiple packages (removable or solderable)
- Is compliant with multiple segments requirements (IoT and Industrial)

Standard package (form factor) evolution:
- 1FF (ID-1) 1991
- 2FF (Mini) 1996
- 3FF (Micro) 2003
- 4FF (Nano) 2012
- MFF2 (DFN8 5x6) 2016
## ST4SIM complete portfolio

### Internet of Things

<table>
<thead>
<tr>
<th>Basic SIM &amp; eSIM</th>
<th>Optimized and Cost effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST4SIM-100x</td>
<td>ST4SIM-100S</td>
</tr>
<tr>
<td></td>
<td>ST4SIM-100M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Crypto 5G SIM &amp; eSIM</th>
<th>Advanced secure communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST4SIM-110x / ST4SIM-111x</td>
<td>ST4SIM-110M / ST4SIM-111M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GSMA eSIM</th>
<th>Scalable &amp; interoperable solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST4SIM-200x</td>
<td>ST4SIM-200S</td>
</tr>
<tr>
<td></td>
<td>ST4SIM-200M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GSMA 5G eSIM</th>
<th>5G, Scalable &amp; interoperable solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST4SIM-201x</td>
<td>ST4SIM-201S</td>
</tr>
<tr>
<td></td>
<td>ST4SIM-201M</td>
</tr>
</tbody>
</table>

[-25°C, +85°C]   [-40°C, +105°C]
Next gen product for IoT

Scalable security solution for full product life cycle

User friendly

Power Sustainability Innovation

MEMS
LED
Super cap
Modem/WiFi / Zigbee/BT…
Dynamic NFC Tag
STSAFE100A
EAL5+
Page EEPROM/FLASH
No App
STM32
Sensors
Page EEPROM
STM32
I2C
STM32
LED
STM32
Modem/WiFi / Zigbee/BT…
Dynamic NFC Tag
Page EEPROM/FLASH
STSAFE100A
EAL5+
ST25R
ST4SIM
EAL5+
Our technology starts with You