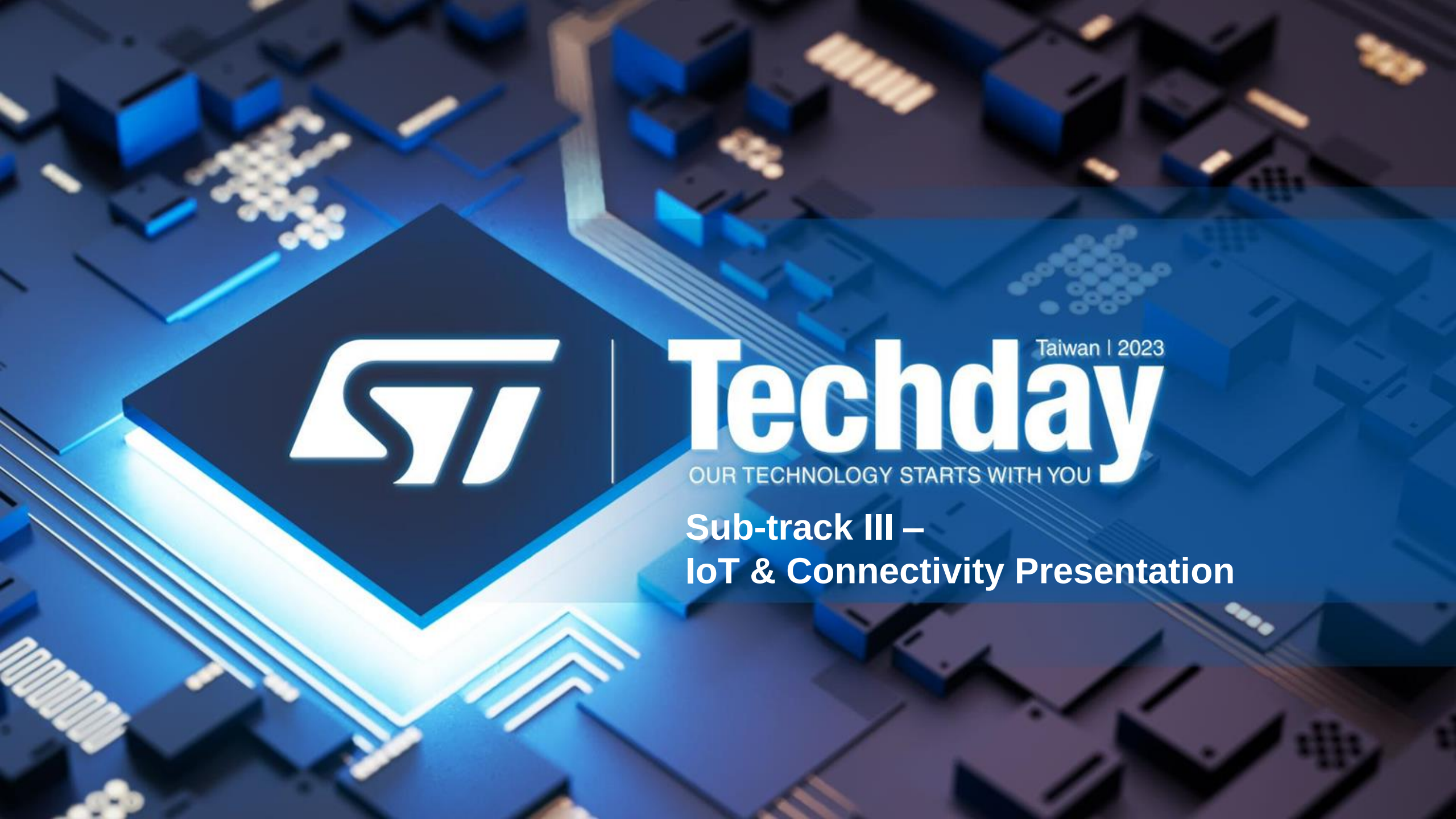


Sub-track III –
IoT & Connectivity Presentation

life.augmented

Connected security for IoT

Kenneth Huang
Marketing Manager
STMicroelectronics

Connected security portfolio

Worldwide sales & marketing offices

Manufacturing and personalization sites across the globe

EEPROM

36%	Market share in 2022*
20+	Billion units shipped to date
32Mbits	Smart Page EEPROM inventor

* Based on actual 3Q'22 Omdia Nov'22

NFC Tags & Readers

20%	Market share in 2022**
34+	NFC Forum certified products
60+	Ecosystem: demos, boards and software package

** Based on ST internal analysis Feb'23

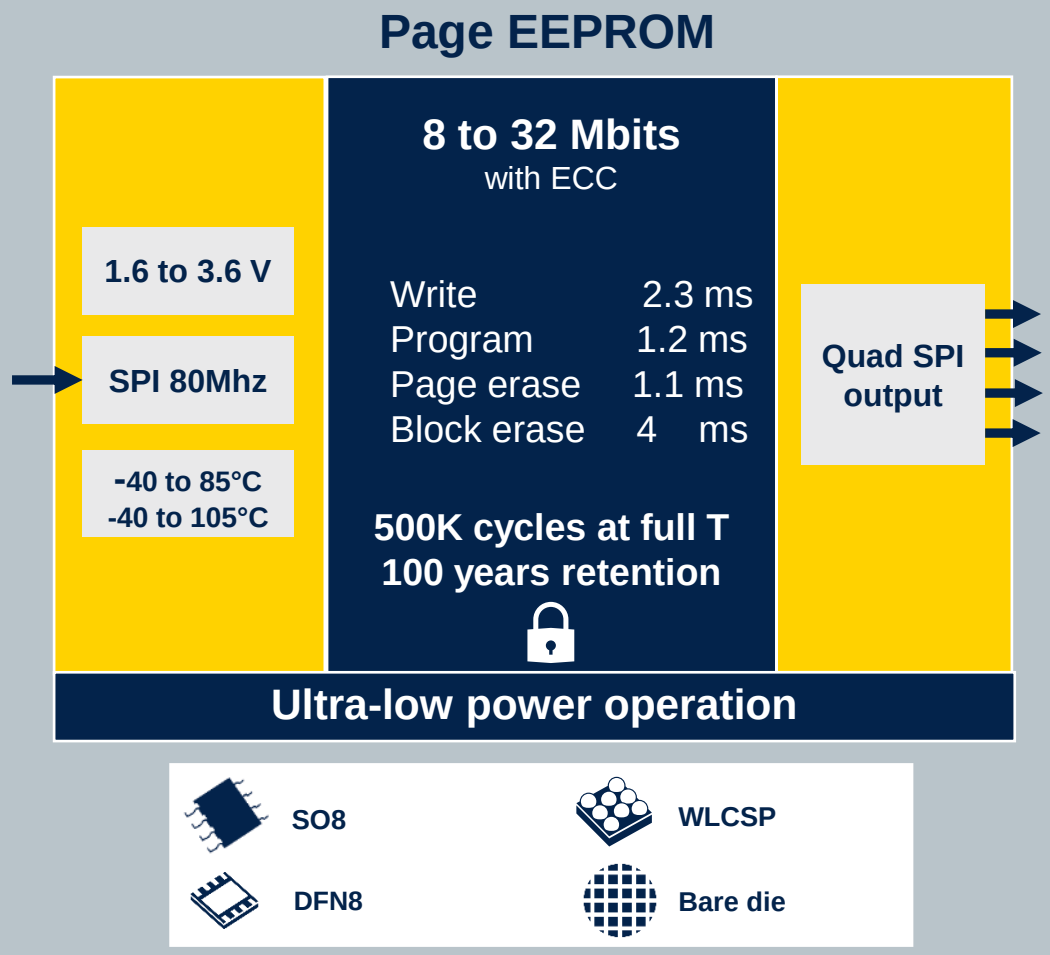
Secure MCUs

20%	Market share in 2022***
15+	Billion units shipped to date
30+	Years of experience in security

*** Based on WSTS Feb'23

life.augmented

Page EEPROM ID card



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

life.augmented

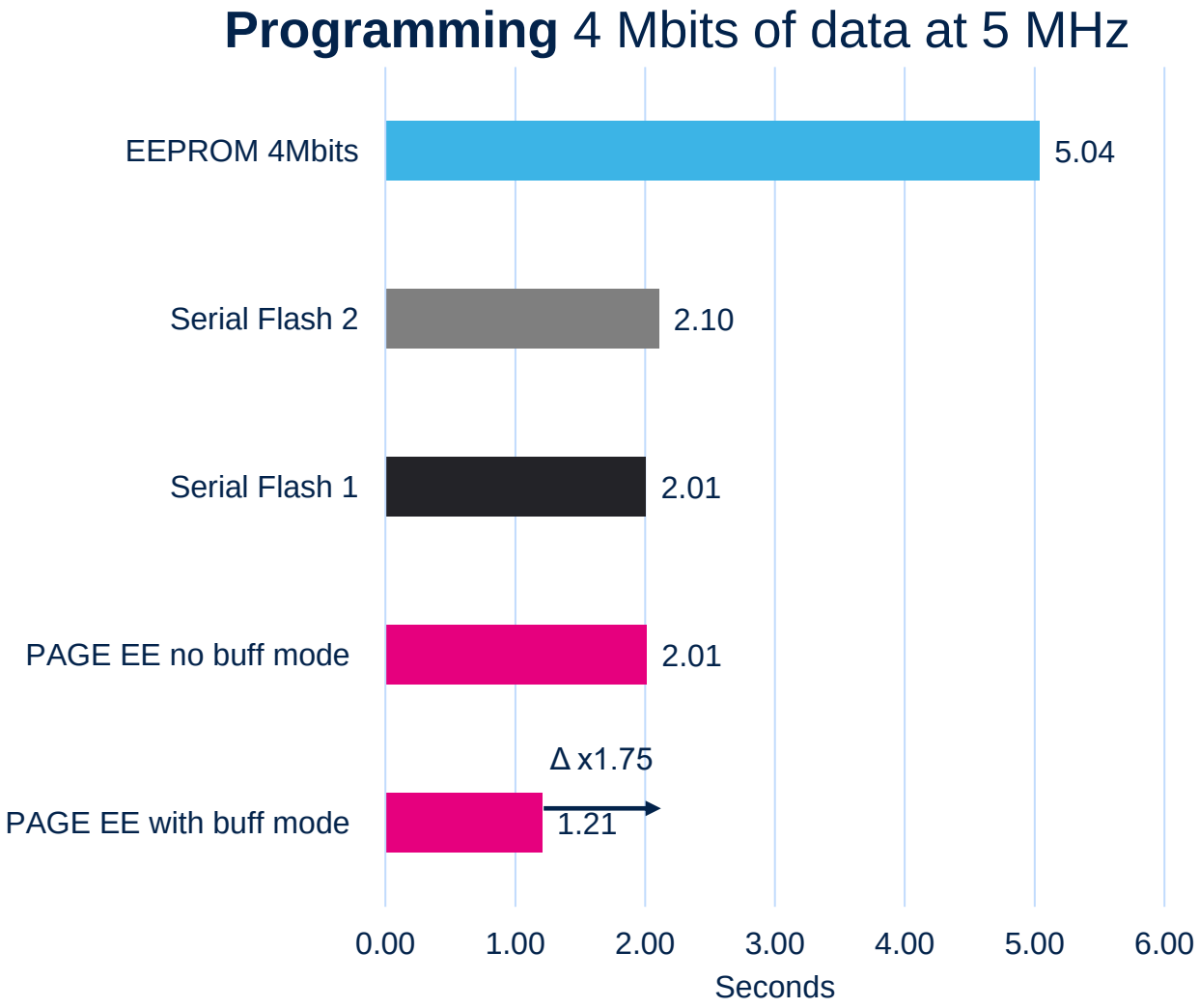
Page EEPROM specifications
SPI interface & power consumption

Voltage range	1.6 to 3.6V	SPI interface
Temperature range	-40 to +85°C and 105°C	
Wake up latency	30 µs	
SPI interface	80 MHz SPI single/dual/quad output	
Standby current	15 µA	Ultra low power
Deep power down	0.6 µA	
Read current	< 500 µA	
Erase current	<1mA	
Program current	< 2 mA	
Write current	< 1.5 mA	
Peak current control	< 3 mA	

Note : typical values

life.augmented

Manufacturing



- **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

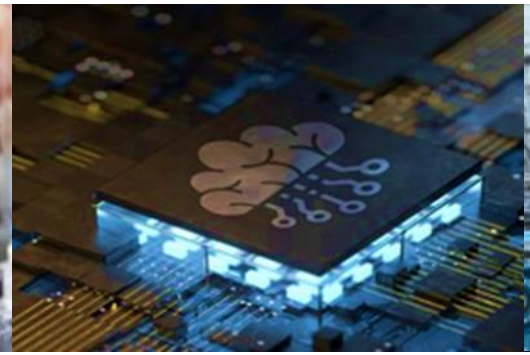
Ultra-low power

- 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

life.augmented

NFC non-smartphone products

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

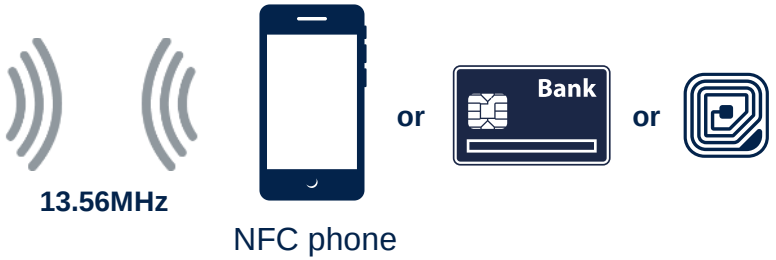
Tags

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

Dynamic tags

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

Readers

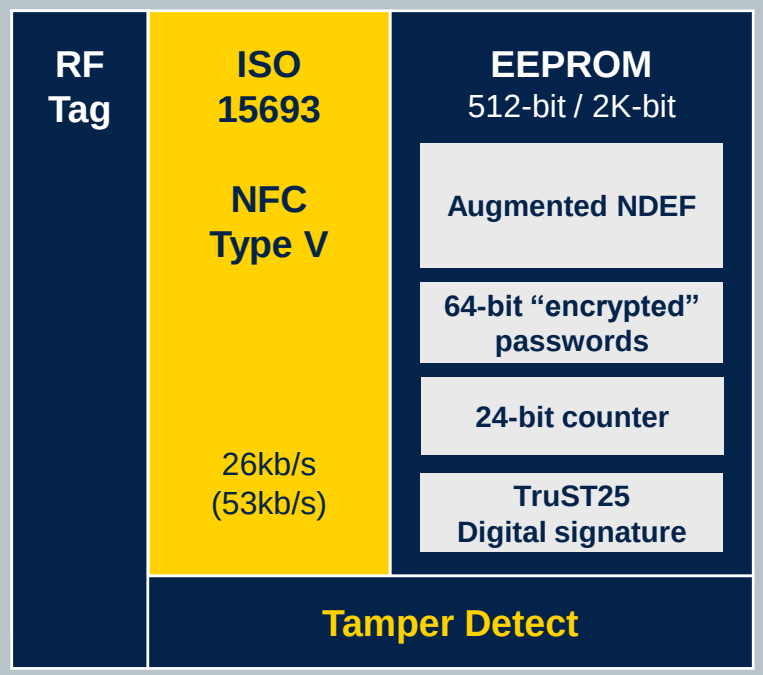


life.augmented

ST25TV512C / 02KC ID card

ST25TV512C / 02KC

F9P



FPN5

SBN12 / SBN075
Die form, sawn and Bumped inkless 8" wafer, 120µm/75um thickness

Use cases

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

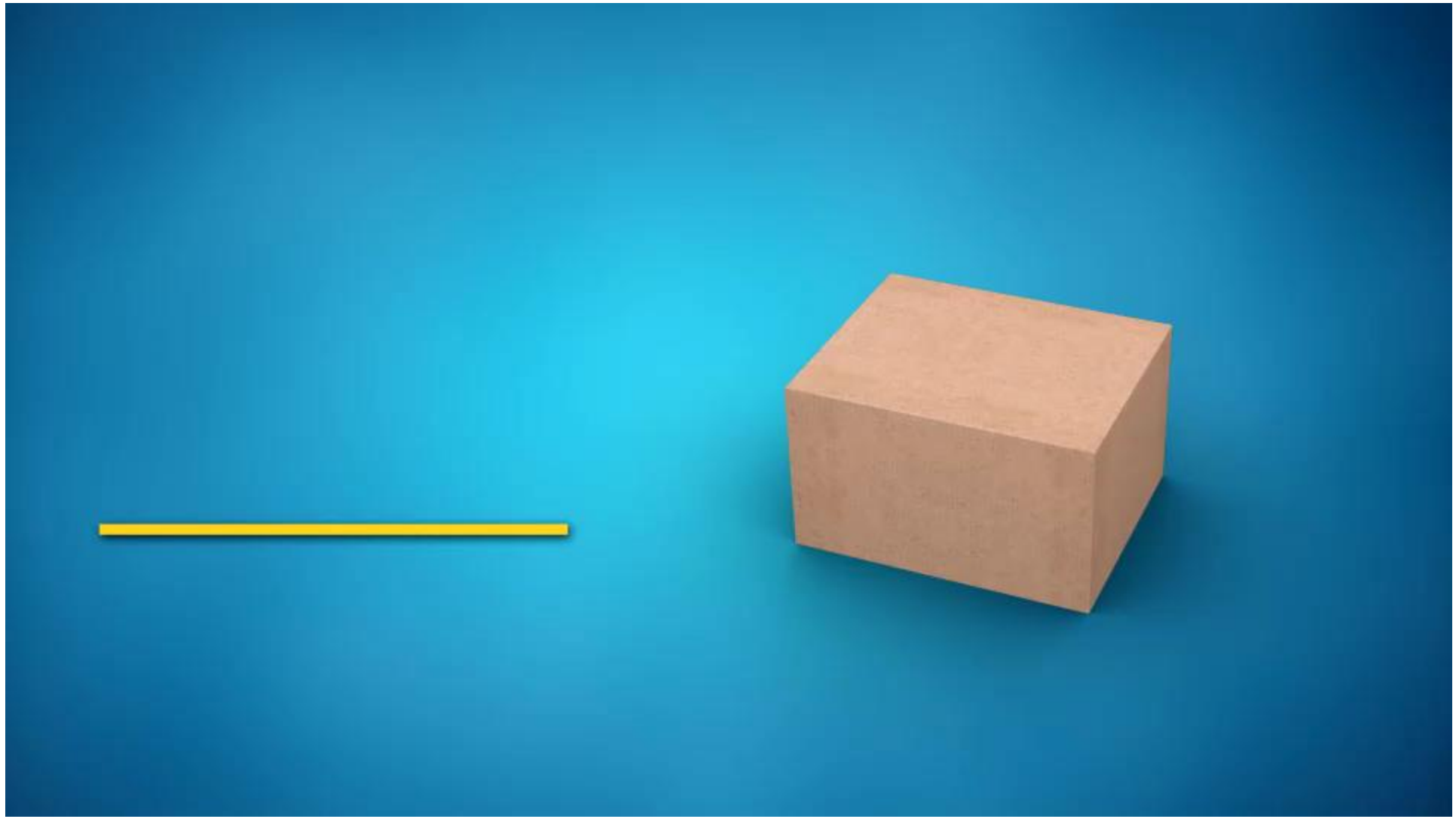
Key Features

- **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

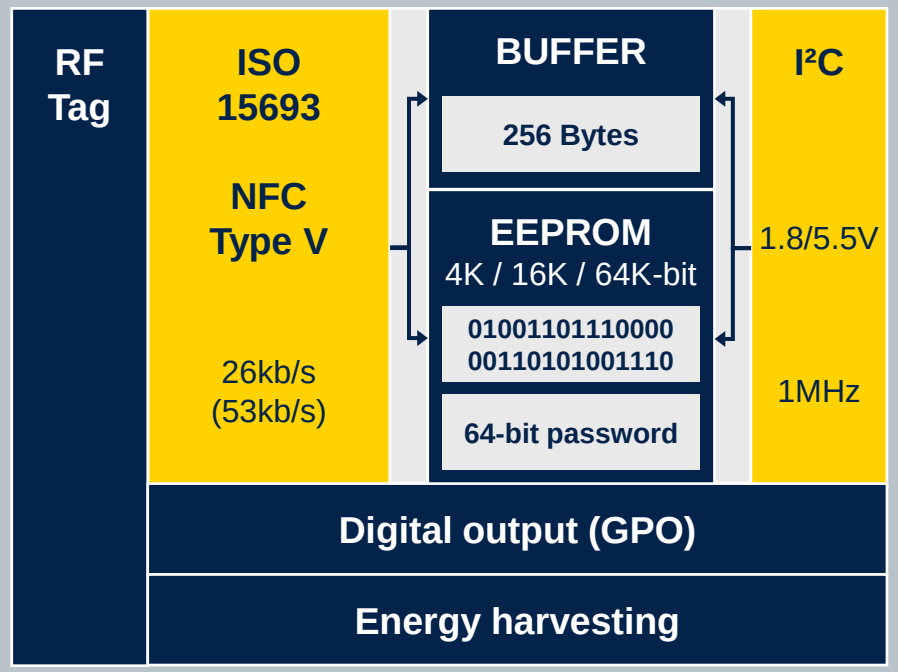
ST25T temp protection tag



life.augmented

ST25DV-I2C-EVO
enhanced dynamic NFC Type 5 tag

ST25DV04KC / 16KC / 64KC



 SO8

 FPN8

 WLCSP10

 TSSOP8

 FPN12

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…)

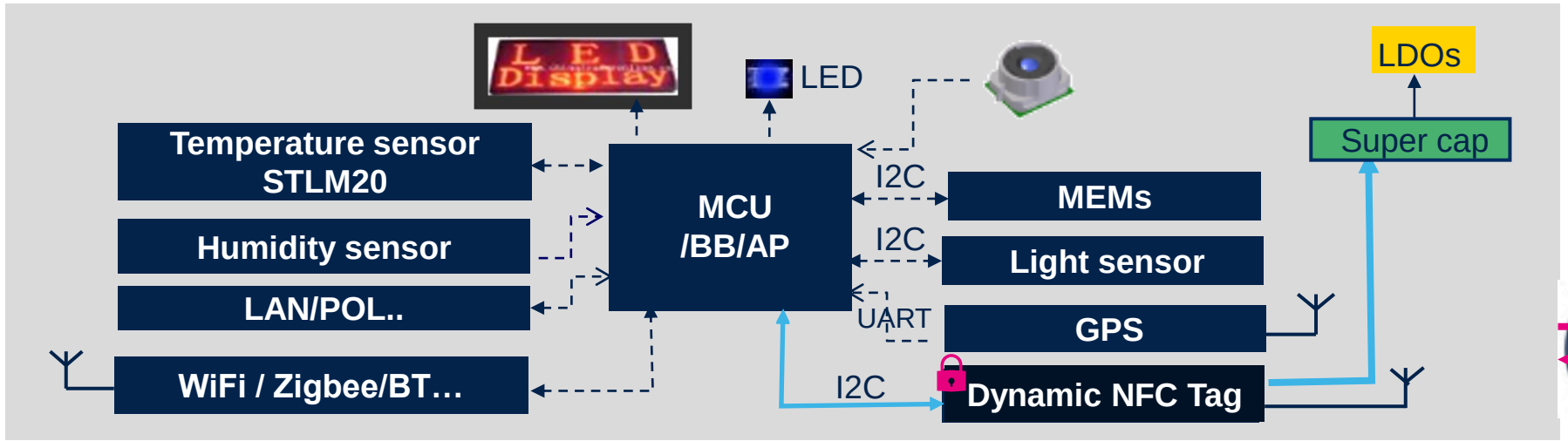
Key benefits

- 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!

Metering /Lighting | Appliances | Consumer /Wearable | Automotive | Medical | Cold Chain /Logistics | Industrial /Robot



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

- 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

life.augmented

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

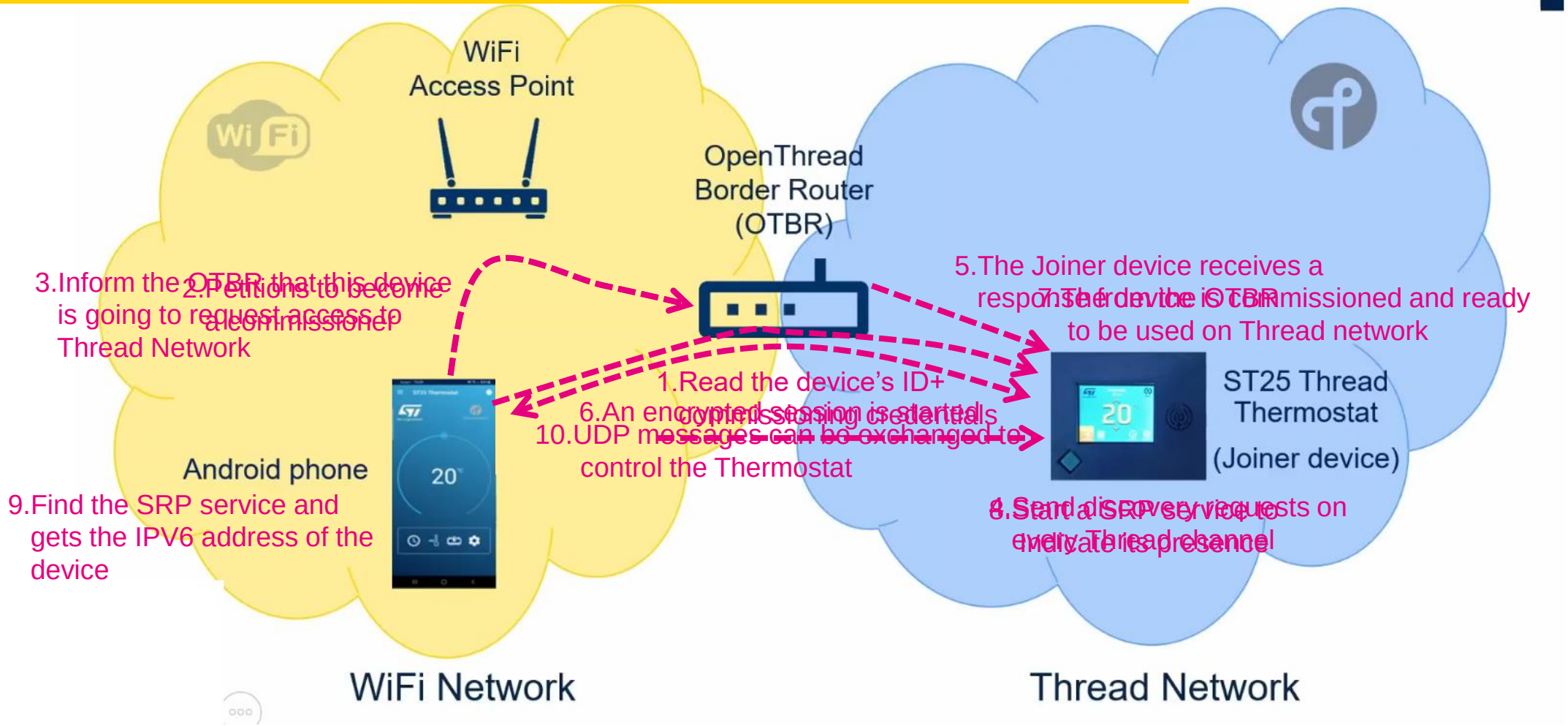
From your device cradle to grave

life.augmented

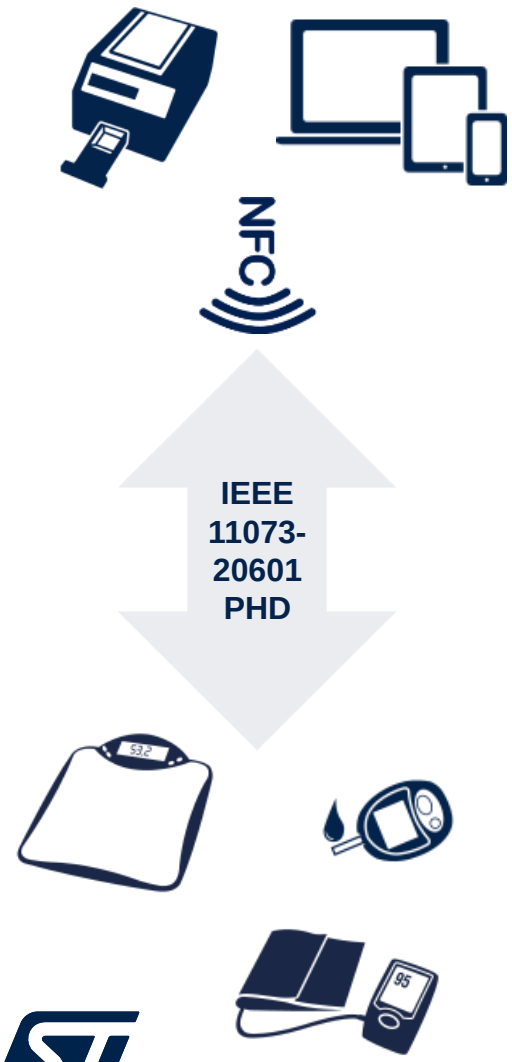
Thread commissioning over NFC

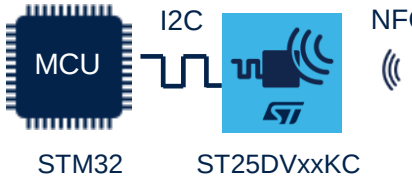
Use NFC to simplify the thread commissioning procedure by one tap

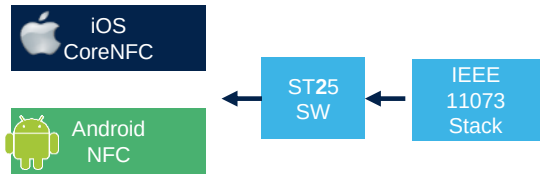
Synopsis

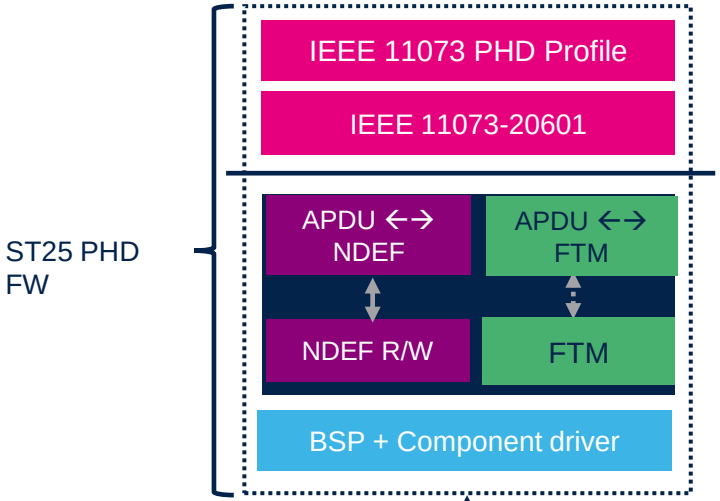


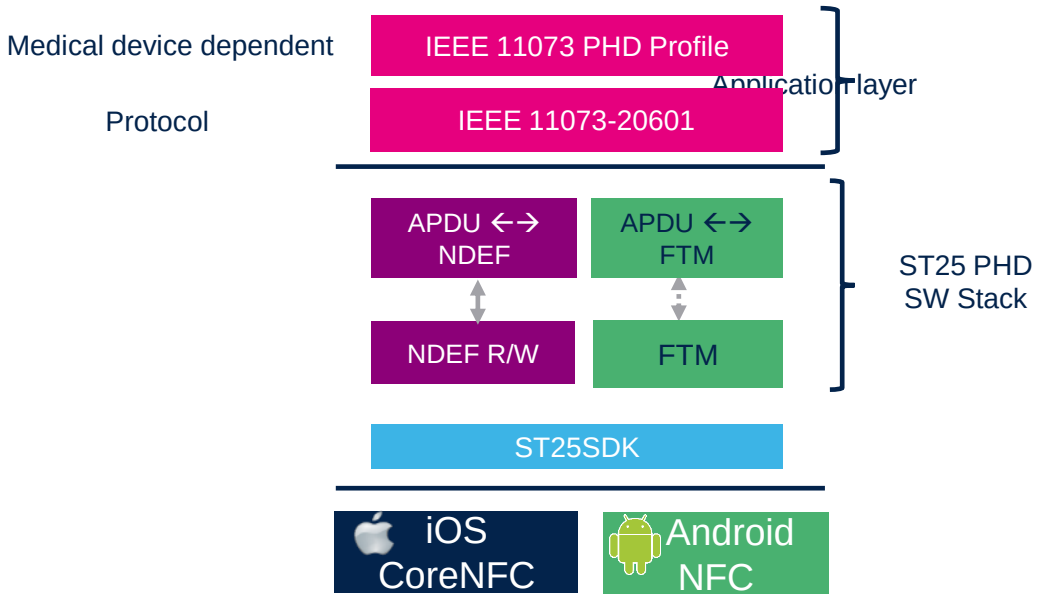
ST25 for IEEE 111073 PHD











life.augmented

Next gen UFD/SSD

Next Gen

ST25DV for lock / unlock management

life.augmented

ST25D applications

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

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

www.st.com/st25d

Batter user experience

Tape and download an app
Wireless pairing
Data download/data -log

Secure locked/unlocked

Use an NFC phone to lock or unlock the private device with size and cost concern

Energy harvesting

Active E-paper panel/LED/low power device w/o on-board power

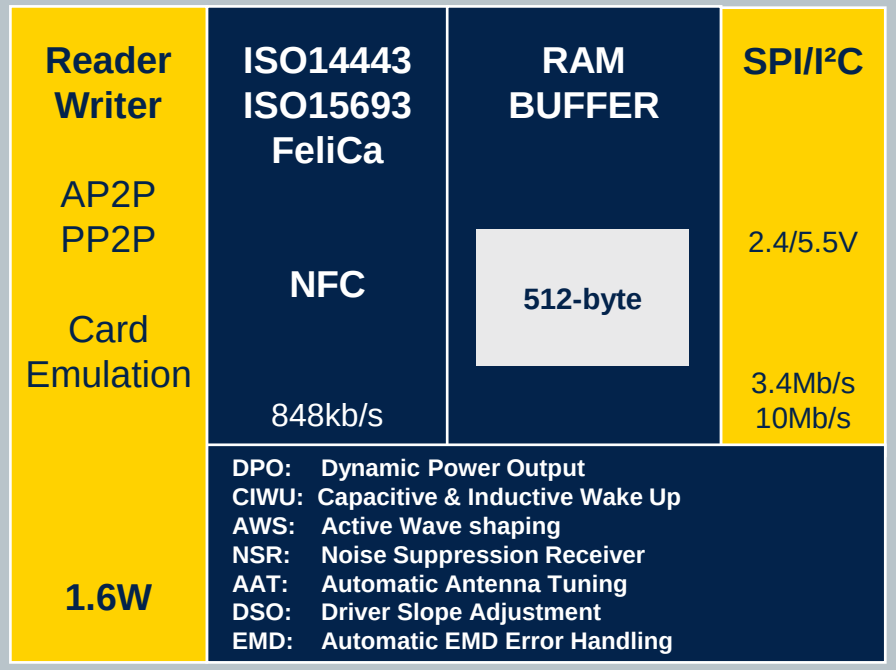
Parameter setting

Data download / FW upgrade in production

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

ST25R3916
high-performance NFC universal device & EMVCo reader

ST25R3916



QFN32
Wettable flank

WLCSP

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…

www.st.com/st25r

Payment

Contactless Payment

Car access

Digital key for Door handle
Start engine

Access control

Smart lock
Building / Hotel Access

Authentication

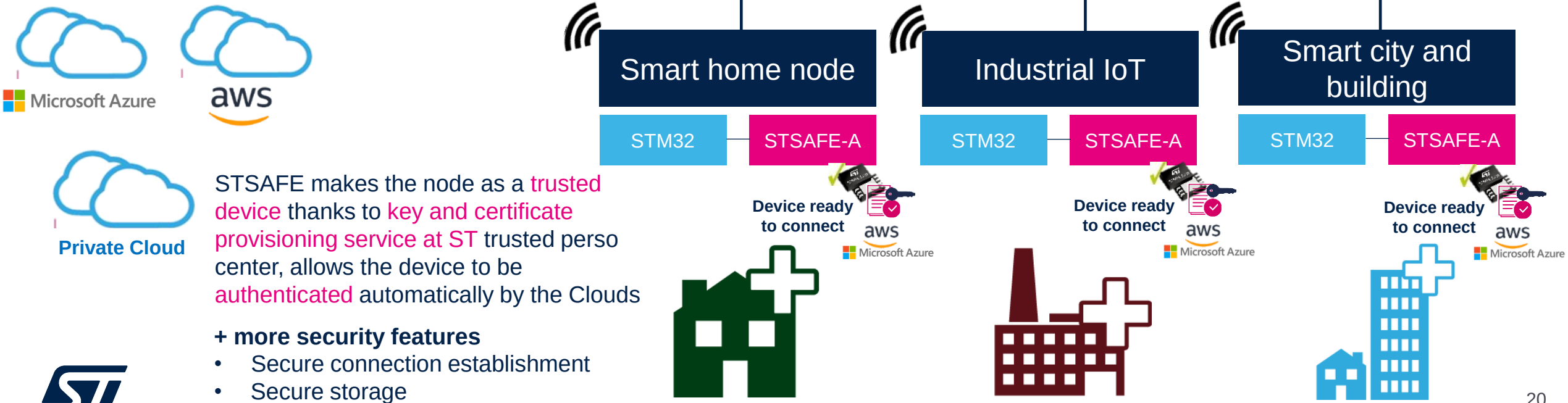
Battery monitor for E-scooter
Accessory management for printer, Air filter, medical test kit

STSAFE-A110 @ IoT

Threats come when massive IoT devices connected

Major driver: IoT security awareness

What is our target ?



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

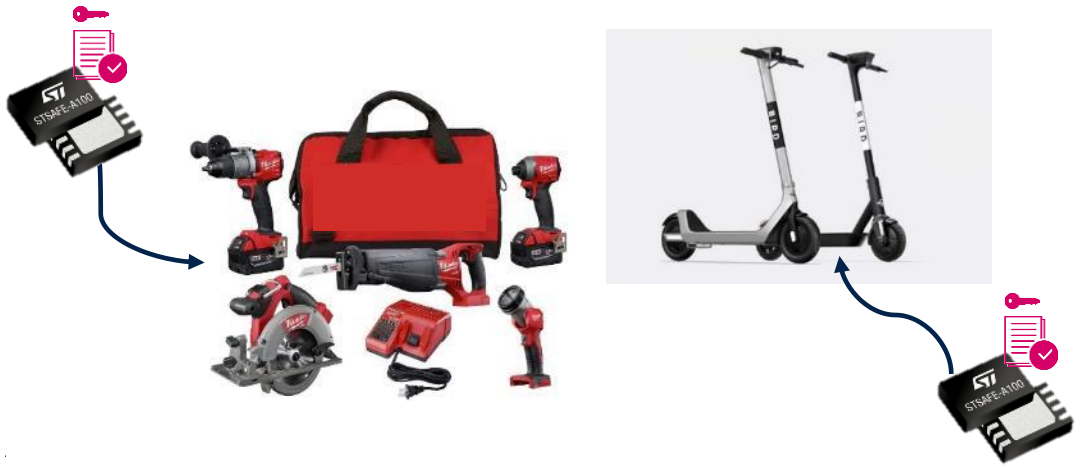
+ more security features

- Secure connection establishment
- Secure storage
- Secure FOTA

life.augmented

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

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



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:

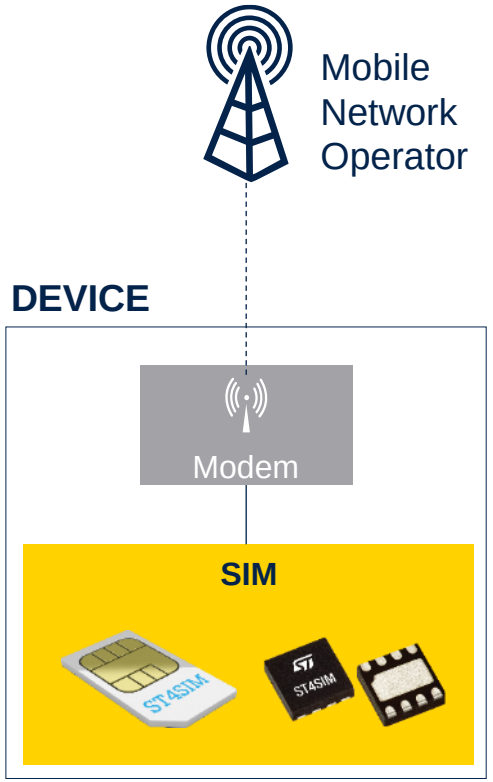
STSAFE-A110 and Secure Cloud Connectivity, a new way to automate device registration™

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

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

life.augmented

ST4SIM complete portfolio

	Internet of Things	Industrial
		
	ST4SIM-S	**ST4SIM-M**
Basic SIM & eSIM ST4SIM-100x	Optimized and Cost effective	
	ST4SIM-100S	**ST4SIM-100M**
Crypto 5G SIM & eSIM ST4SIM-110x / -111x	Advanced secure communication	
	ST4SIM-110S / ST4SIM-111S	**ST4SIM-110M / ST4SIM-111M**
GSMA eSIM ST4SIM-200x	Scalable & interoperable solution	
	ST4SIM-200S	**ST4SIM-200M**
GSMA 5G eSIM ST4SIM-201x	5G, Scalable & interoperable solution	
	ST4SIM-201S	**ST4SIM-201M**
	[-25°C, +85°C]	**[-40°C, +105°C]**

life.augmented

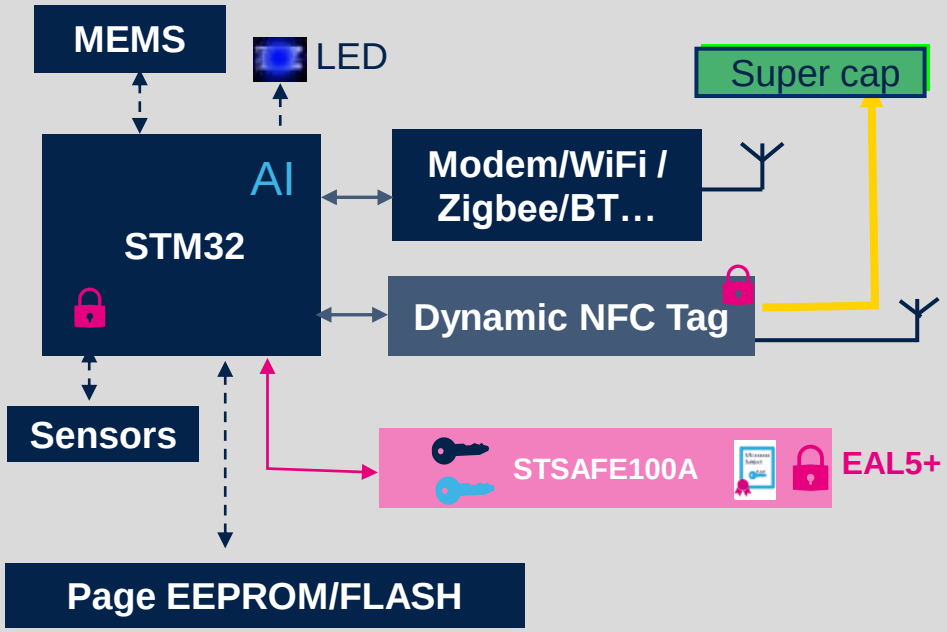
Next gen product for IoT

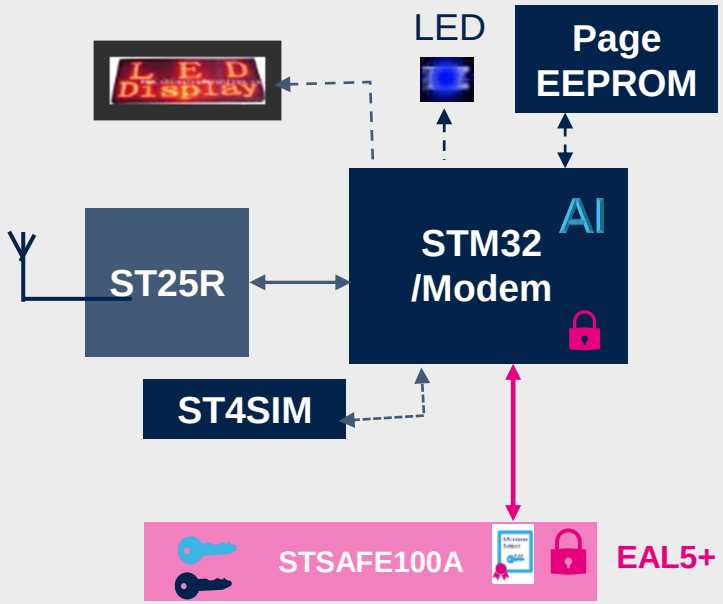
Scalable security solution for full product life cycle

Power Sustainability Innovation

User friendly

No App





life.augmented

Our technology starts with You

life.augmented