life.augmented

Connected Security:

Enhancing protection and convenience in the digital age

In the news


life.augmented


HACKADAY
ROOT ON THE PHILIPS HUE IOT BRIDGE
Anatomy of an IoT hack
FBI: Security researcher admitted to hacking planes 15 to 20 times while in-flight
HOW THE INTERNET OF THINGS GOT HACKED
THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE
IoT and liability: Who pays when things go wrong?
Osram smart lighting flaw lets hackers breach home Wi-Fi
Why the next big data breach could come from the heating

Objects Counterfeiting Issue

Counterfeiting is a growing threat affecting companies worldwide

Because consumables and peripherals are basic but can be costly, they are more likely to be counterfeited

Consequences for companies can be particularly significant, in terms of:

- Revenue loss
- Quality
- Brand image

life.augmented

Companies' business model evolution trend

From a traditional business model…

Companies' traditional business model is to sell goods in shop

- One-time income
- No feedback from customers' experience

…To a service-based approach

Companies expand this model to sell extra recurrent services

- To ensure recurrent revenue
- To make customers more captive
- To get direct feedback from customers

Thanks to new technologies

- Connected objects, among which sensors & actuators
- Data processing in Cloud
- Artificial Intelligence

When the customer pays for the service, the quality expectation is higher

Authentication as The Solution

What if we could provide an **authentication solution** that would allow to distinguish genuine objects from counterfeit **AND** securely connect objects to their cloud?

This **authentication solution** would allow to protect:

- Revenues
- Product quality
- Brand reputation
- The behavior of a system based on connected objects
- The privacy of the data exchanged between the objects and the cloud

How can ST help to enhance protection and convenience in your products

life.augmented

More than 30 years of expertize in security

2024
Introduction of advanced technologies

2017 - 2022
First eSIM integration in smartphone & Personalization sites GSMA certification

2009
First EAL6+ Common Criteria certification on contactless secure MCU

1995
First Smartcard IC supporting Public Key Cryptography

1984
First MCU-based Smartcard IC for banking applications

Continuous innovation

Advanced secure technologies

Post-quantum cryptography, secure provisioning, secure enclave

Securing all your applications

- **Banking & ID** (Payment, ID, passport, health cards, transport & PayTV)
- **Brand protection and computer** (Consumable & TPM for computer)
- **Mobile secure transactions** (eSIM, eSE, NFC, secure wearable)
- **Secure application digitalization** (Payment, transit, car access)
- **IoT & industrial** (utilities, smart home, automation, public sector)
- **Smart driving** (eSIM, eSE)

Consumer goods

Providing secure solutions: PKI (Public Key Infrastructure), TPM (Trusted Platform Module) brand protection, anti-piracy & anti-fraud

Smartcard

Supporting all the manufacturers for banking, ID, SIM, transportation & PayTV applications

life.augmented

Best-in-class HW security

Tamper-Proof certified solution

Non-invasive attacks material & IP theft

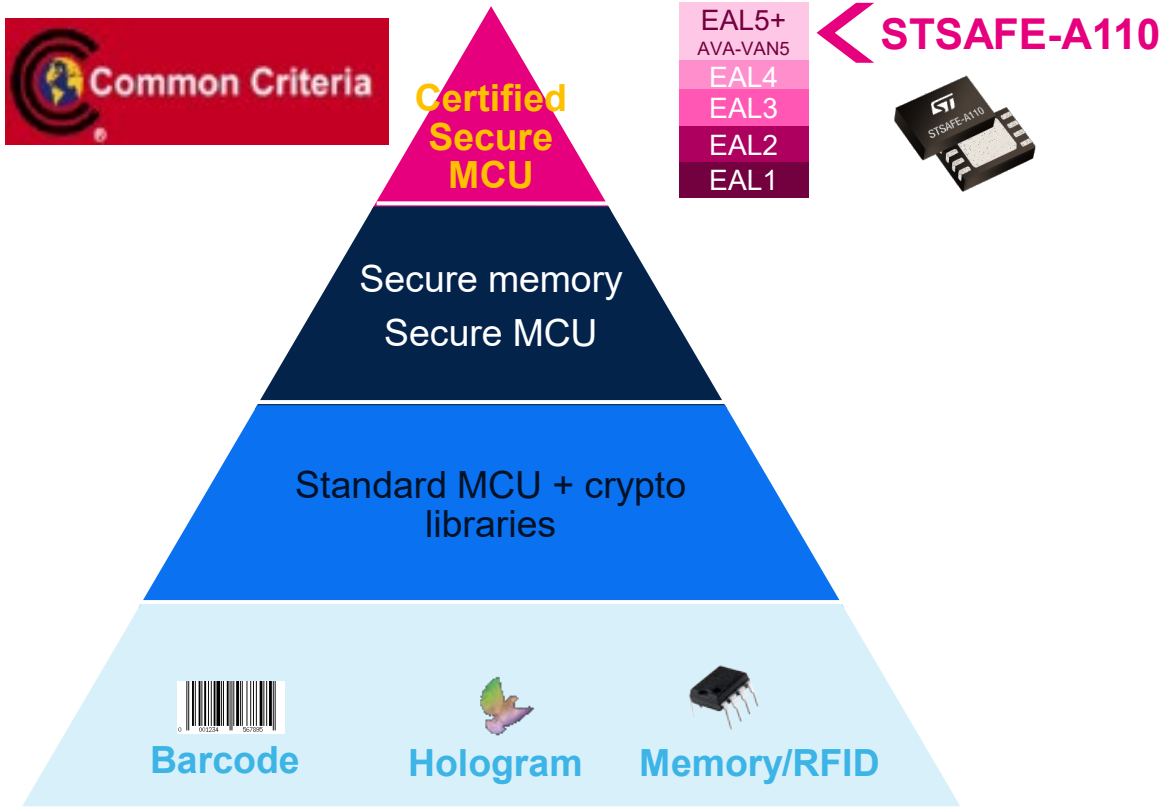
- Secure manufacturing and development environments

Semi-invasive attacks fault injection

- Dedicated architecture and design
- Hardware and Software countermeasures

Invasive physical attacks

- Shields
- Intrusion detectors
- Obfuscation



When security is considered in customer design…

How to

manage my key at 3rd party?

develop the code in secure manner?

do provisioning with trust?

make sure the secret safe during lifecycle?

life.augmented

STSECURE Turnkey Solution: Solving Security Concerns

How to

manage my key at 3rd party?

develop the code in secure manner?

do provisioning with trust?

make sure the secret safe during lifecycle?

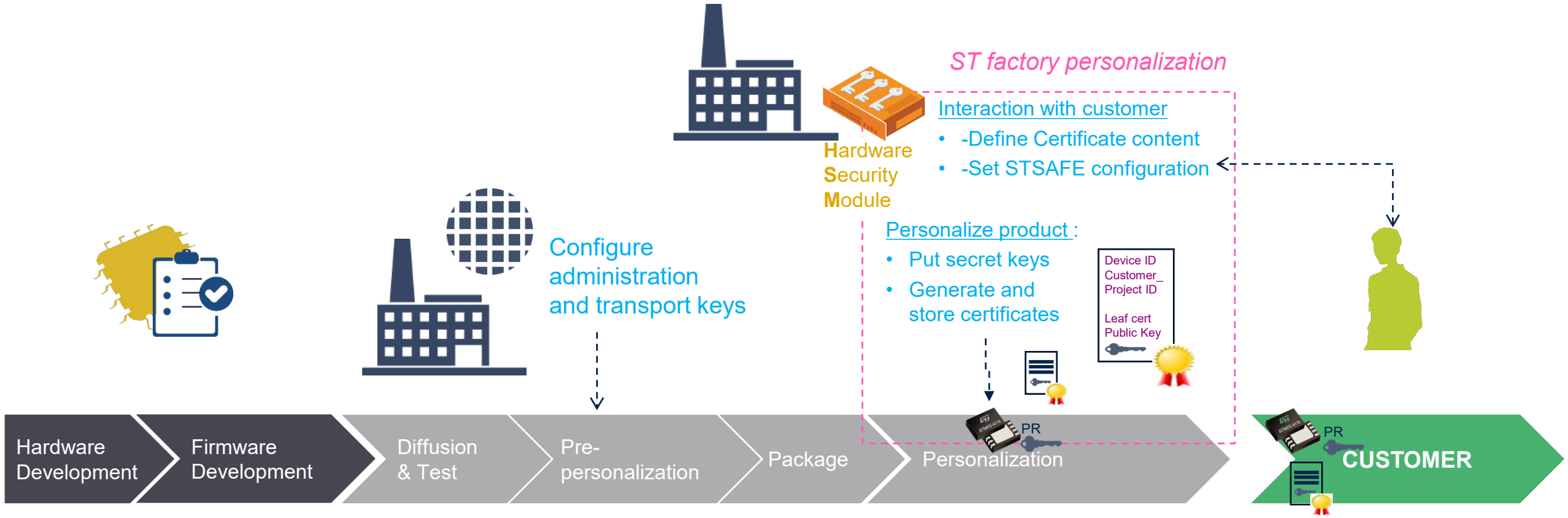
Turnkey solution

- Private keys and certificates loading at ST in a secure and certified environment
- Secure FW developed by ST
- Secure element certification done by ST
- Demonstration codes provided by ST
- Customization service could be selected

life.augmented

STSAFE-A production with personalization by customers at ST secure factory

Secure Environment



Flow and facilities approved by independent security authorities:

Common Criteria GSMA EMVCo

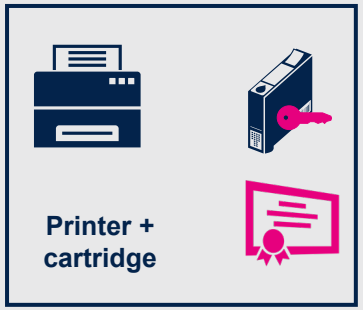
MOQ=5Ku

life.augmented

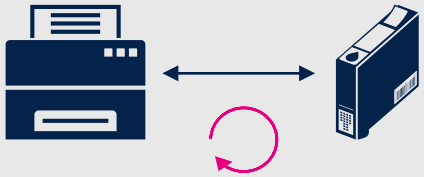
STSAFE-A Offering

Brand protection

Verify a consumable or a peripheral is genuine

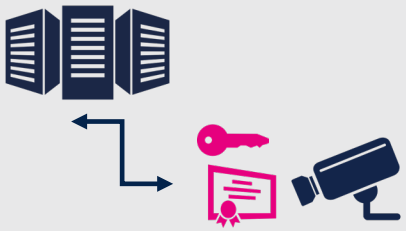


Control the number of consumable use

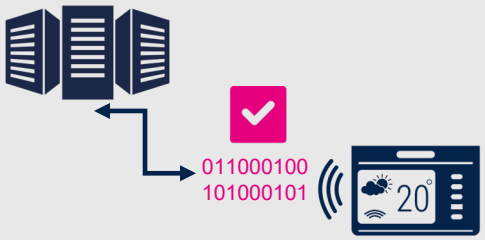


Security for connected device

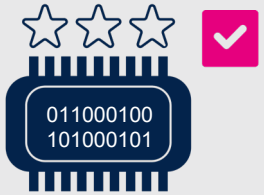
Verify device is genuine or its access rights



Ensure confidentiality & integrity of exchanged data



Ensure embedded firmware integrity



life.augmented

STSAFE-A features & applications

Best-in-class embedded Secure Element (eSE)

CC EAL5+ certified

Key applications

- Smart Home (matter)
- Healthcare
- Power supply (Open Compute Project)
- Metering
- Industrial equipment
- Wireless charging (Qi)

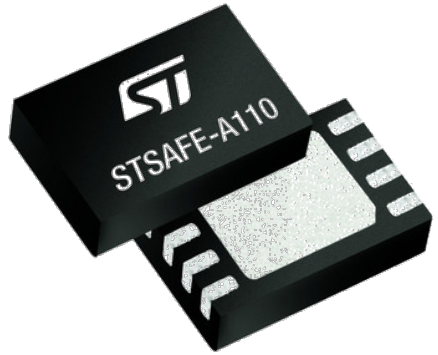
life.augmented

Rich feature set

- Authentication with personalized certificate
- Secure connection establishment
- Secure data storage
- Signature verification

Best-in-class hardware

- Highly secure MCU, CC EAL5+ AVA_VAN5 certified
- 6kBytes EEPROM
- 30 years data retention, 500kcycles
- Temperature range: -40 to 105°C
- 1µA consumption in hibernate mode



Personalization

- Customer certificate and keys personalization at ST secure factory

Introducing the SIM & eSIM concept

From the removable SIM to the soldered and interoperable eSIM

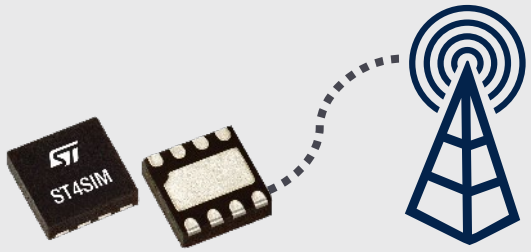
Classical SIM Card
Removable

Traditional SIM concept inherited from mobile phone

1 SIM Card = 1 operator

Embedded SIM (eSIM)
Soldered

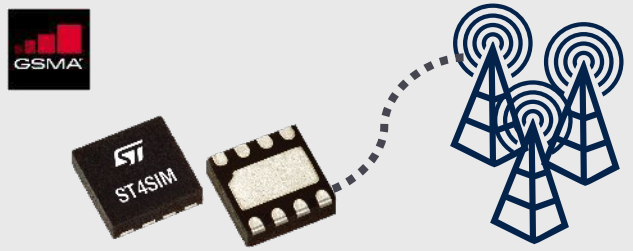
An optimized footprint and reliable package as soldered



1 eSIM Card = 1 operator

GSMA-certified eSIM
Soldered & Interoperable

Possibility to change remotely the operator without replacing the SIM



1 eSIM Card = X operator

life.augmented

ST4SIM ecosystem

ST4SIM component

- IoT and Industrial grade HW
- Multiple form factor
- SIM / eSIM SoC configuration
- GSMA eSIM certified and interoperable

+ Pre-loaded connectivity from partners

Telecom Operator

User

Application

Connectivity management

Connectivity platforms

Telecom Operator

TRUPHONE

wireless logic

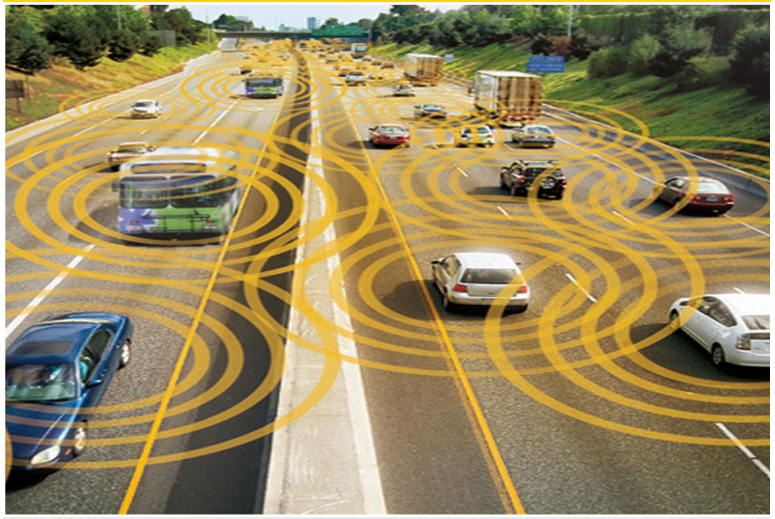
Complete ecosystem with

- **SM-SR:**
  Subscription Manager Secure Routing
- **SM-DP:**
  Subscription Manager Data Preparation

life.augmented

What is next?

eSIM for M2M
Available today



- Regular ETSI/3GPP M2M
- GSMA SGP.02 3.2 in volume production
- GSMA SGP.02 4.2 available for 5G

Single / Multi operators

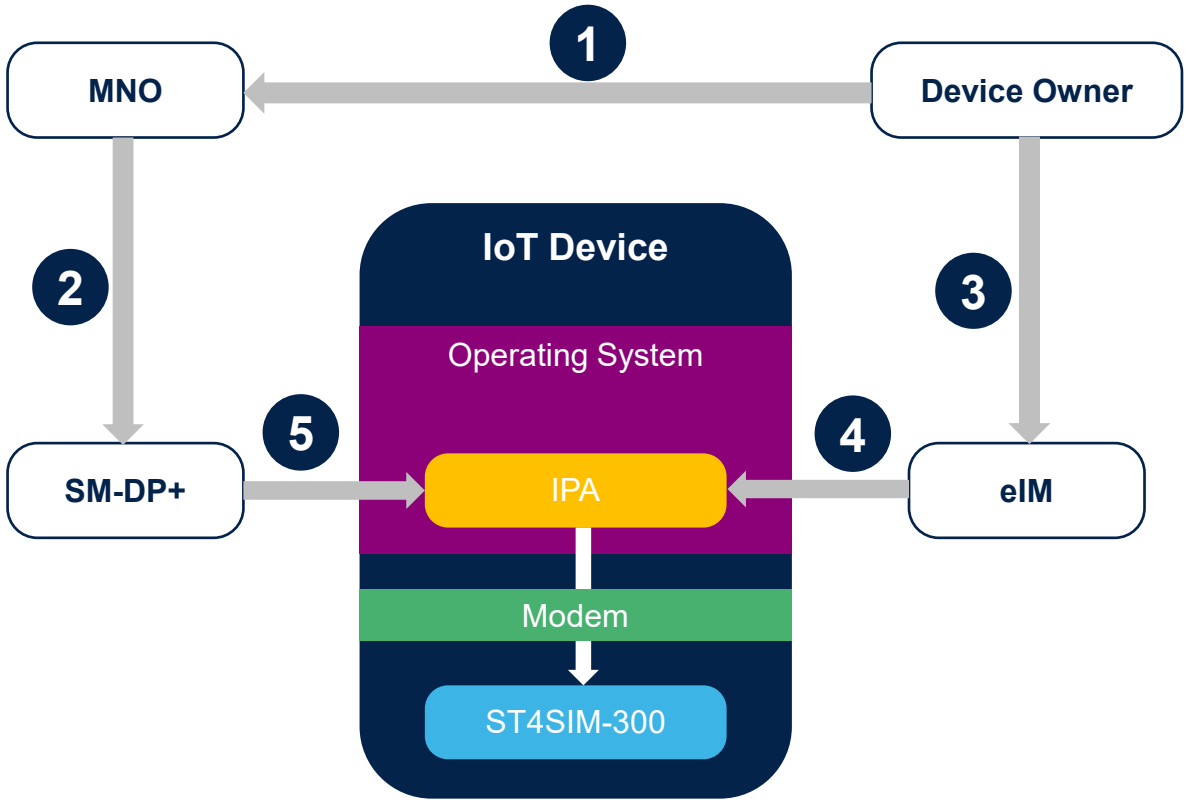
eSIM for IoT
GSMA standard in preparation

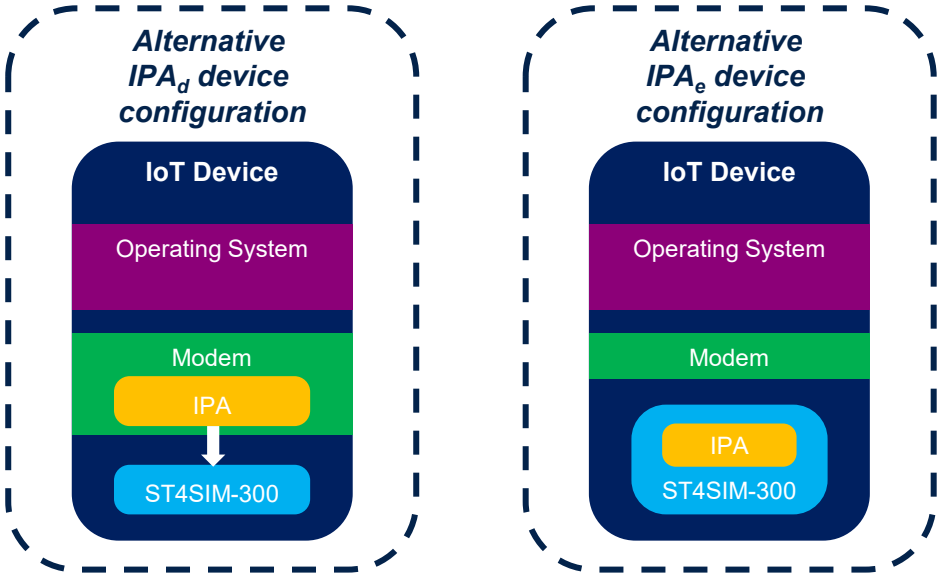
- GSMA technical spec SGP.32 scheduled in Q1 ’23
- Full deployment expected in 2024
- Ease the remote provisioning

Multiple operators

life.augmented

ST4SIM-300: eSIM for IoT workflow

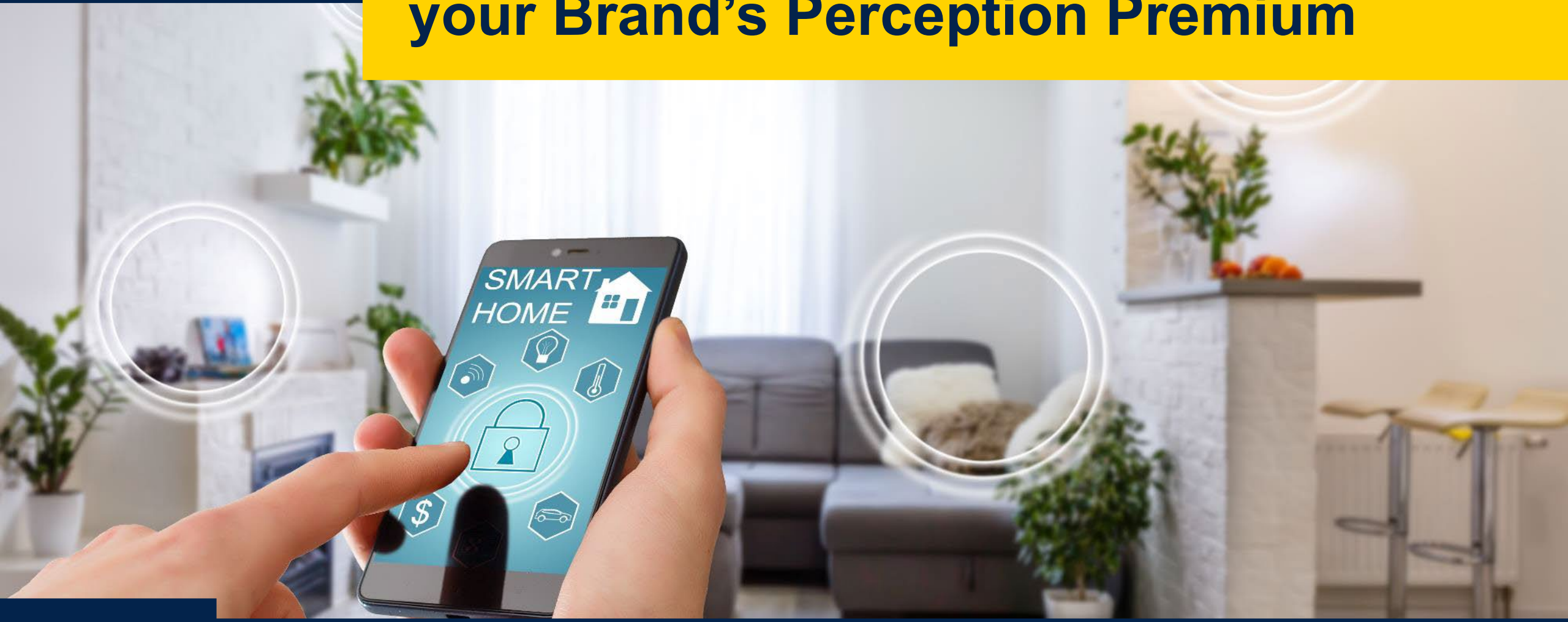




1. Device owner order profile from MNO
2. MNO Order profile on RSP
3. Device owner push “download” command to eIM
4. eIM push information to device
5. Device start downloading profile from RSP

life.augmented

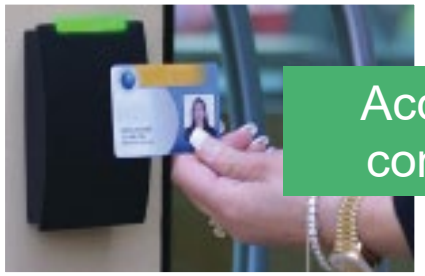
Convenience is the New Key to make your Brand's Perception Premium



life.augmented

NFC main benefits and applications

Device pairing



Access control

Contactless Payment

short range

Inherently secure

facilitates setup of wireless technologies (BT, Wi-Fi…)

standardized

interoperable

NFC

Technology-enabler

intuitive

simple tap

Battery-less

zero-power

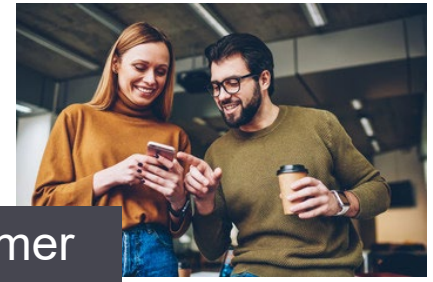
Security-ready

built-in capacities to support secure applications

Identification

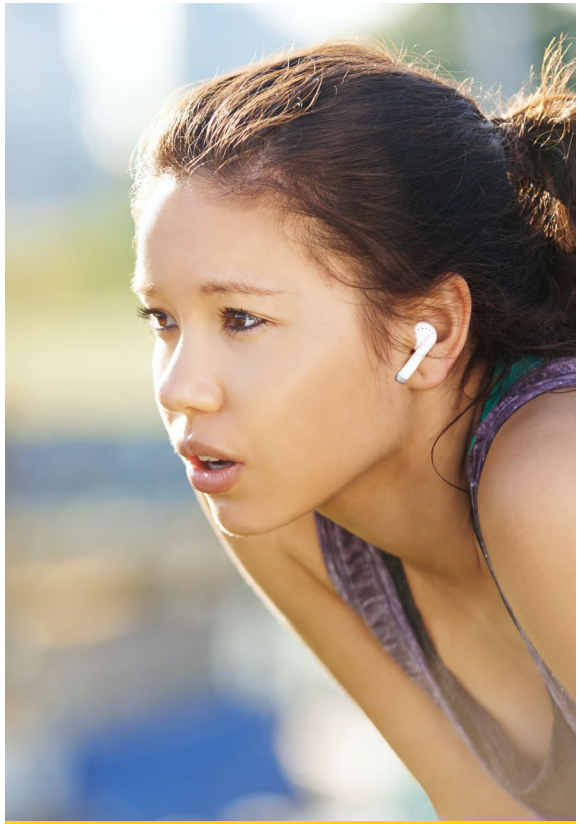
Parameter settings

Consumer interaction



And more…

NFC emerging markets



NFC wireless charging
Earbuds, Stylus, Remotes, Smart glasses

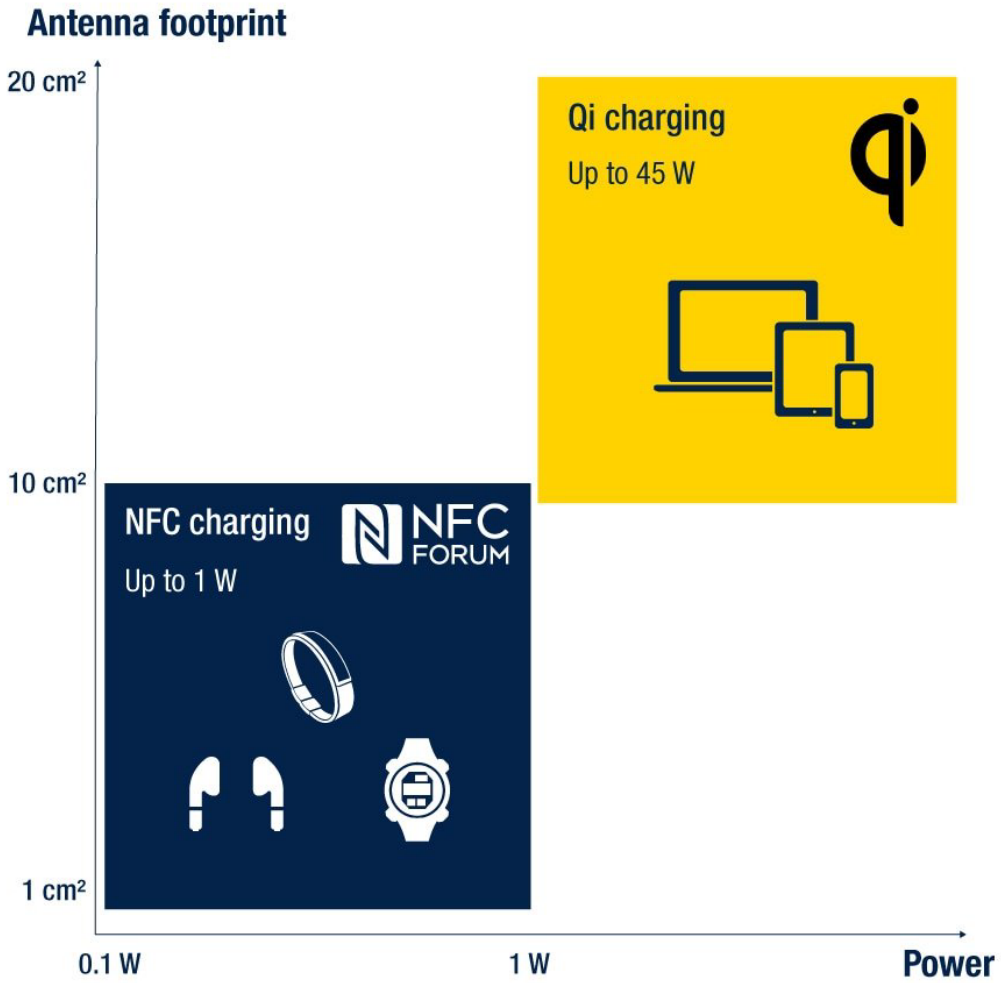
Ki Cordless Kitchen
Blender, Water kettle, Coffee machine

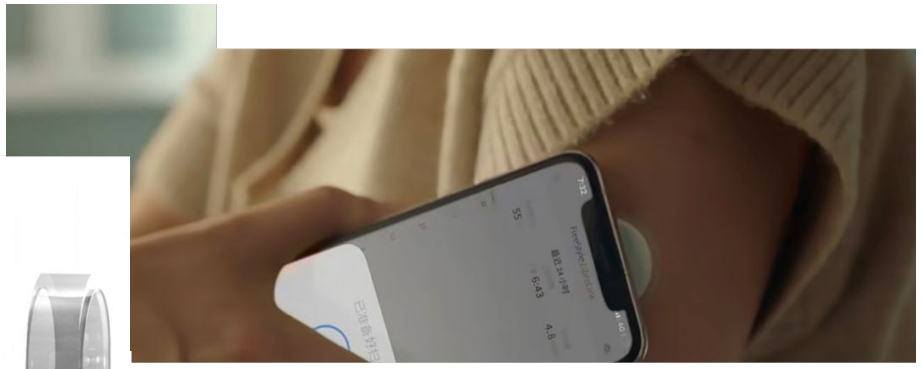
CSA Access Control
Smart locks, gateways, public transport

Commissioning over NFC
BLE, Lora, Thread, Matter, CSA

life.augmented

The trend of NFC Wireless Charging



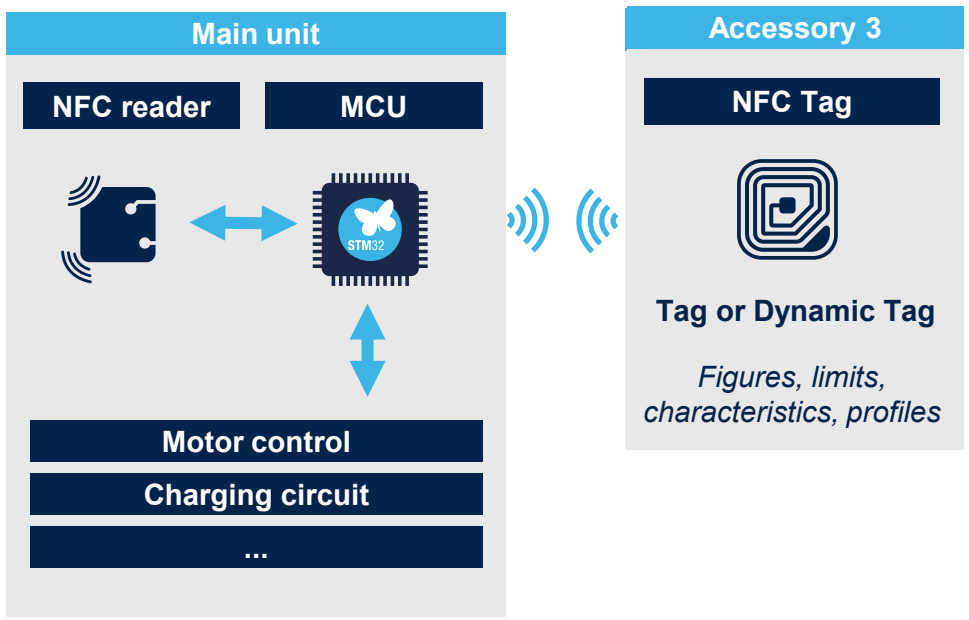


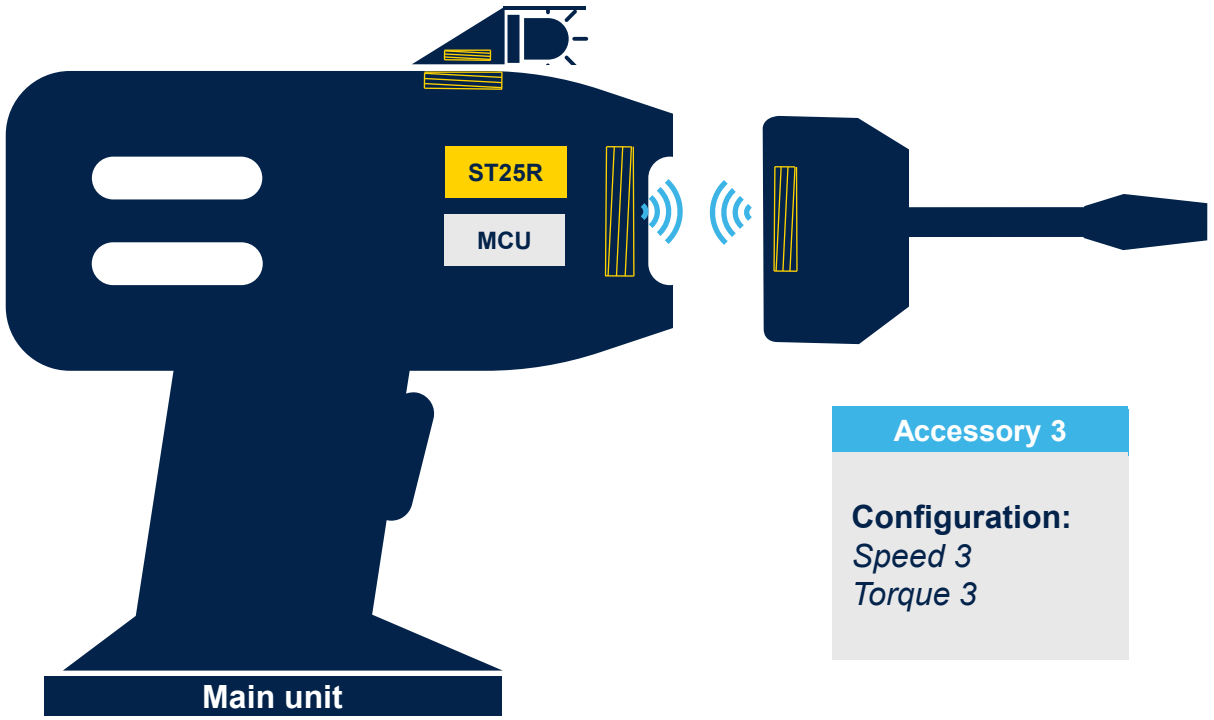
life.augmented

Accessory recognition solution with NFC

Automatic adjustment to new accessory via NFC

Parameters are integrated in the tag, **no preprogramming** of main unit necessary





Commissioning over NFC

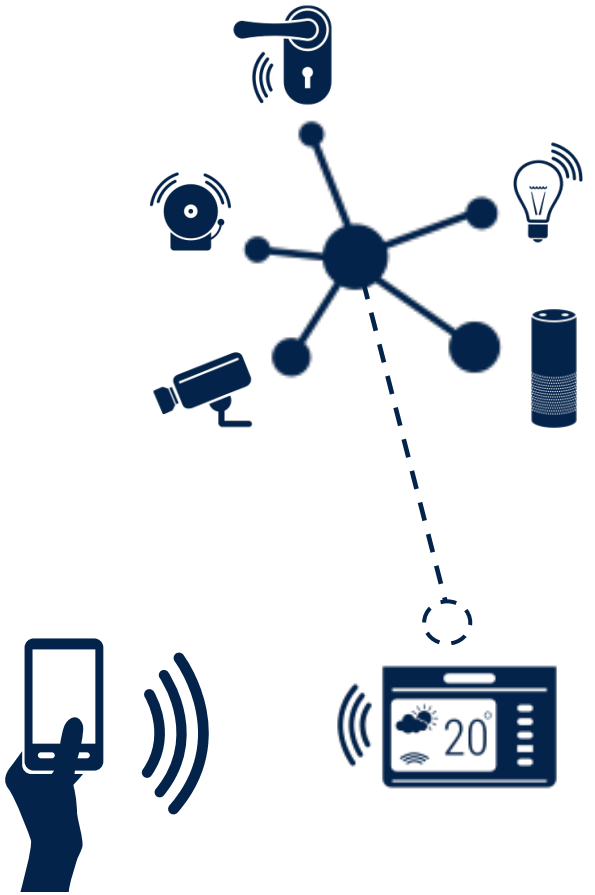
Multiple networks available:

- BLE for smart devices
- Lora network for several miles distance
- Thread network for home
- etc…

Whatever the network, commissioning is generally done as follows:

Given a **device** provisioned **with unique information** (ID, keys…) at manufacturing stage

1. Get **Device Information**
   - Through NFC tag, email, documentation, website, QR code…
2. **Authentication**
   - New device to be allowed to “enter” on the network
3. **Joining / Onboarding**
   - Once allowed, device can join
4. **Activation**
   - Some devices need to be activated once on the network



life.augmented

Offering flexibility with EEPROM memory solution

Leadership
Worldwide presence, #1 ranking and 35% market share

Innovation
Ultra-low power Page EEPROM technology

Availability
Wide product portfolio, ready to pick

Differentiation
Service, Performance & Quality

Long term commitment
In-house technology and efficient manufacturing

life.augmented

EEPROM extended portfolio

Serial EEPROM	Page EEPROM
NEW 256Kb 512Kb 1Mb 2Mb 4Mb	NEW 8Mb 16Mb 32Mb
2Kb - - - - 16Kb 32Kb 64Kb 128Kb 256Kb 512Kb 1Mb 2Mb	
I2C, SPI, Microwire 85°C, 105°C, 125°C, 145°C SO8N, TSSOP8, DFN8, DFN5, WLCSP, Bare die	QUAD SPI 85°C, 105°C SO8N, DFN8, WLCSP
Standard 35% market share*	Automotive 60% market share*
	New market → Demand creation

life.augmented

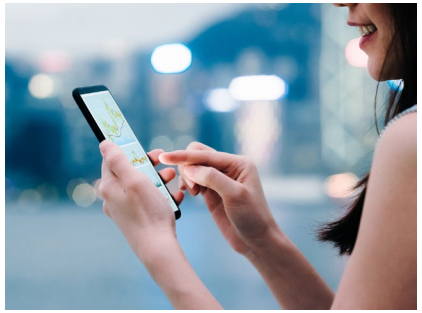
*Source: Omdia Competitive Landscaping Tool March 2023

Connected Security applications

for Everything

Everywhere

for Everyone



Mobile Security & Memory

M2M Cellular Connectivity

Payment

Identity & Transport

Trusted & Connected cars

Consumer authentication

Brand Protection

Industrial
authentication & convenience

IoT
authentication & convenience

Consumer & Healthcare
convenience

life.augmented

Our technology starts with You

Find out more at www.st.com

life.augmented