life.augmented

ST25TA-E
Mint your business

ST25

life.augmented

Solutions for NFC / RFID Tags & Readers

ST25

ST25 SIMPLY MORE CONNECTED

ST25TA-E main market segments

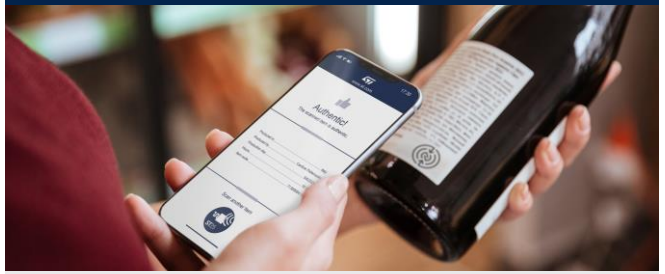
Luxury

Apparel

Jewelry / Watch

Handbag

Wines & spirits

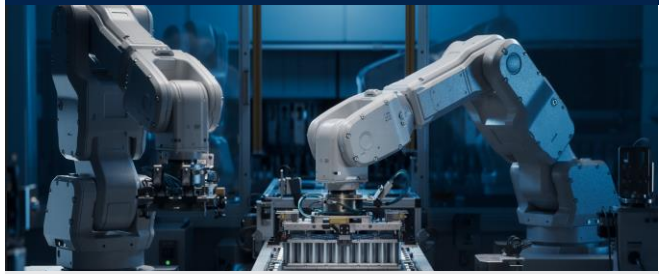


Premium bottle

Art

Artwork

Industrial / Medical



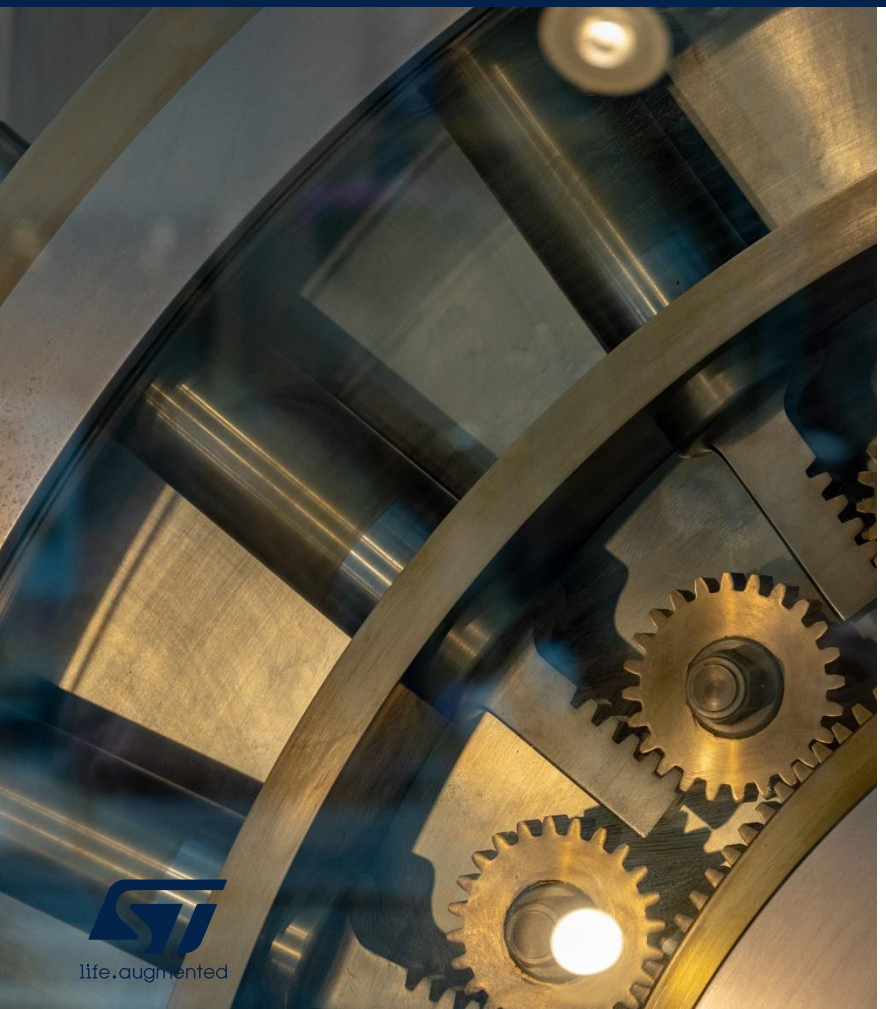
Tool maintenance

life.augmented

ST25TA-E overview

Innovative NFC tag type 4 compatible with blockchain technology

68 pF chip capacitance



Brand protection

- Asymmetric ECC cryptography engine
- Edge TruST25™ digital signature (on-chip ECDSA)
- TruST25™ digital signature (off-chip ECDSA)
- Unique keypairs by chip (2 slots)
- Password & lock file mechanism

Standard compliance

Near Field Communication CERTIFIED™

SESIP™1

Blockchain

- Compatible with blockchain-based applications
- Flexible key management & infrastructure (public key recovery)
- Aligned with blockchain's pillars: transparent/decentralized/immutable

Additional features

- Augmented NDEF for advanced consumer experience
- General purpose counter – configurable on events
- Privacy modes for GDPR compliancy (Kill & Anonymous)

Available in sawn & bumped wafer

- Thickness: 140 µm and 75 µm

life.augmented

ST25TA-E architecture

RF Tag	ISO/IEC 14443-A	ECC-based crypto	MEMORY
	NFC Type 4 Short range 106kb/s		**NDEF** **ANDEF** **Edge TruST25™ digital signature**

SBN140/075
Die form, sawn and Bumped inkless 12” wafer, 140/75µm thickness

Use cases

- Brand protection, anticloning, product authentication, asset tracking

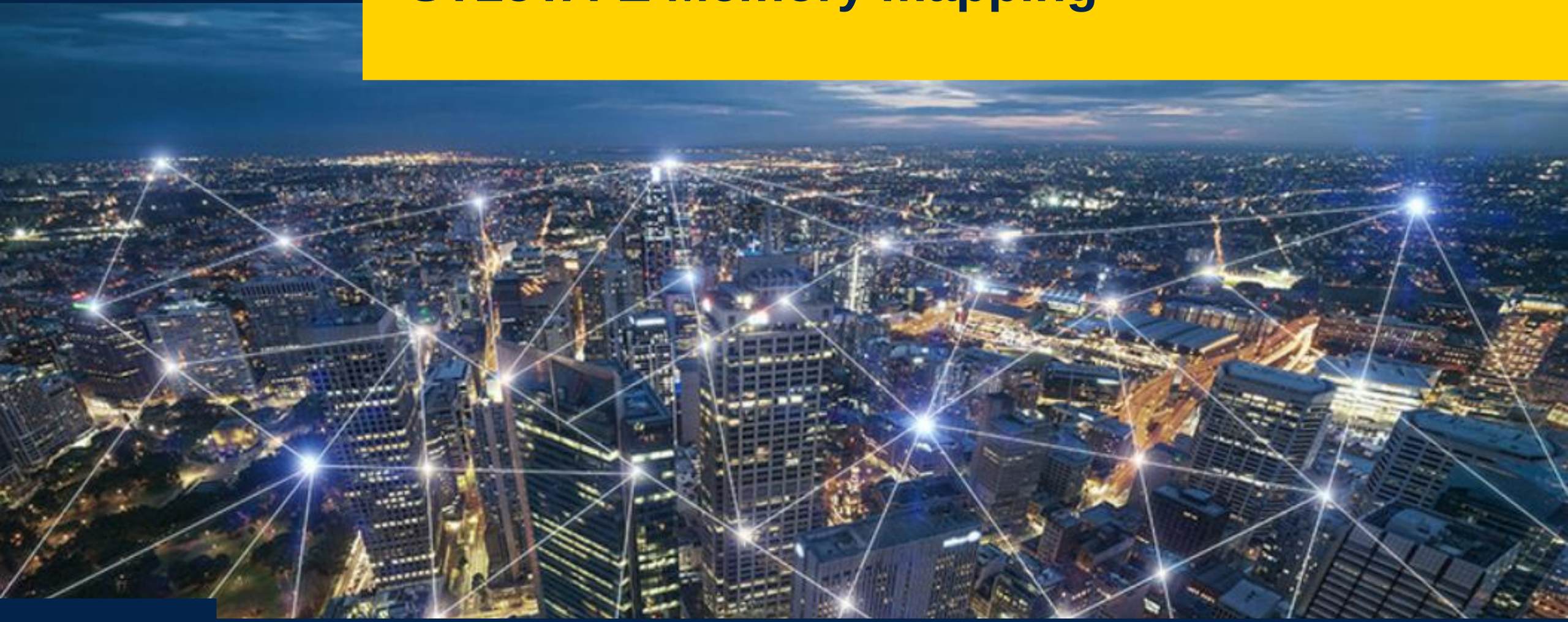
Key features

- **ISO14443-A** and **NFC Type 4**
- Short-range operations, up to **106kb/s** speed
- Data protection using password-based authentication
- **Cloning protection** thanks to Edge TruST25™ digital signature
- Configurable general-purpose counter
- **Privacy-enabled** communication modes
- Tag-related credential appended dynamically to NDEF for consumer engagement (ANDEF)

Key benefits

- **Strong product authentication** thanks to on-chip ECDSA signature
- **Blockchain** compatibility

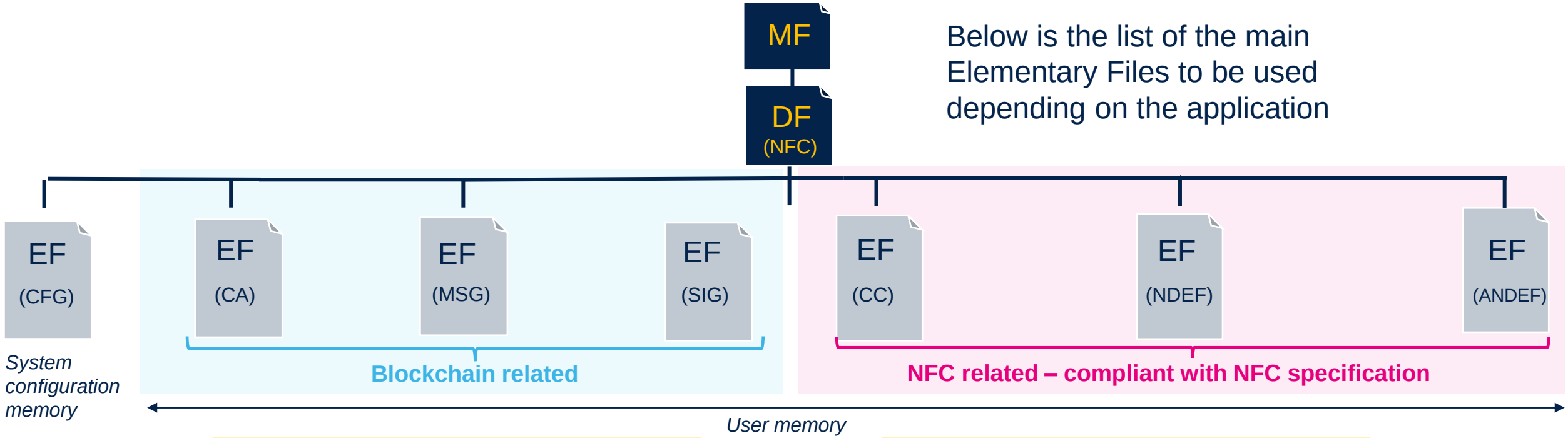
ST25TA-E Memory mapping



life.augmented

ST25TA-E Memory organization

The ST25TA-E memory is organized as a file system



Below is the list of the main Elementary Files to be used depending on the application

- EF : Elementary File
- MSG : Message to sign
- CA : Certificate Authority
- CFG : Configuration
- SIG : Signature

Glossary

- MF : Master File
- DF : Daughter File
- CC : Capability Container
- NDEF : NFC Data Exchange Format
- ANDEF : Augmented NDEF

life.augmented

ST25TA-E file protection

life.augmented

ST25TA-E permanent lock file protection

- Each elementary file can have individual read and/or write access permissions to prevent unauthorized reading from a file / or writing to a file.
- The permanent lock file mechanism that permanently changes the memory content to be readable or writable and makes it impossible to read or change the content after it has been written. This is achieved by changing the file permissions.
- The effect of a permanent lock file operation cannot be reverted.

File name	Permanent read lock	Permanent write lock
CG file	Yes	Yes
CC file	N/A	N/A
NDEF file	Yes	Yes
ANDEF file	Yes	Yes
CA file	Yes	N/A
MSG file	Yes	Yes
SIG file	Yes	N/A

life.augmented

ST25TA-E password protection

- The reversible lock file protection mechanism is based on password-based authentication. This mechanism can restrict use of some ST25TA-E features/commands and prevent read and/ or write access to data stored in each elementary file of user or system configuration memory.
- Each ST25TA-E password is 64 bits length and comes with a default value
- The ST25TA-E devices offer the capability to protect a password against brute-force attacks, thanks to a mitigation that limits the failed password attempt (retry protection)

File name	Reversible read lock	Reversible write lock
CG file	Yes	Yes
CC file	N/A	N/A
NDEF file	Yes	Yes
ANDEF file	Yes	Yes
CA file	N/A	N/A
MSG file	Yes	Yes
SIG file	Yes	N/A

life.augmented

ST25TA-E Augmented NDEF

life.augmented

ST25TA-E Augmented NDEF

Advanced NDEF message services

- The Augmented NDEF feature is a contextual automatic NDEF message service, allowing the tag to respond dynamic content without an explicit memory update.
- Each ANDEF attribute can be enabled/disabled and configured according to the user need
- Native operation : no mobile application required !

✓ All attributes are extracted from the ANDEF message by the server and used inside the application.

✓ Warning can be highlighted in case of doubtful / not expected values.

https://www.server.com	UID + TruST25 Digital signature	UTC	Diagnosis	Custom
	14 Bytes + 68 Bytes	4 Bytes	Up to 10 Bytes	32 Bytes

Static field – NDEF URI

Programmed once into the tag memory

Webserver managed by the customer

ASCII characters

Automatically added at each “tap”

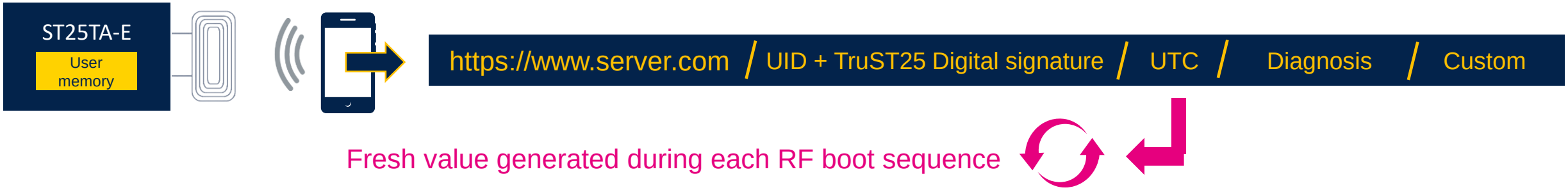
Each attribute can be enabled/disabled

life.augmented

ST25TA-E Unique Tap Code (UTC)

Unique code generator

- The UTC is a 4 digits code generated by the tag itself at each new RF session that makes the ANDEF message (see ANDEF slide) unique and dynamic. It can track up to 455k tap events.
- It benefits from antitearing mechanism ensuring consistency of the counter even in case of electrical problem during its increment.
- The UTC can be configured, activated and read natively.



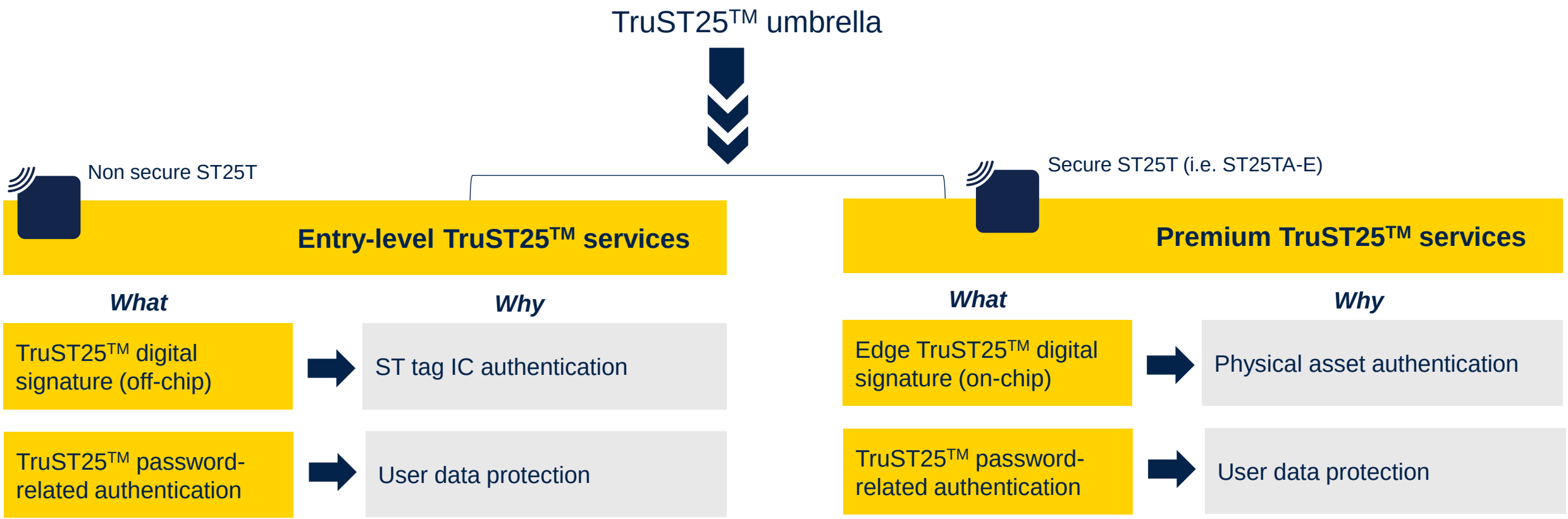
life.augmented

ST25TA-E TruST25™ label

life.augmented

TruST25™ Label

TruST25™ label stands for all security features offered on ST25 NFC tags



life.augmented

Please contact your STMicroelectronics sales office to get more information about the TruST25™ digital signature features

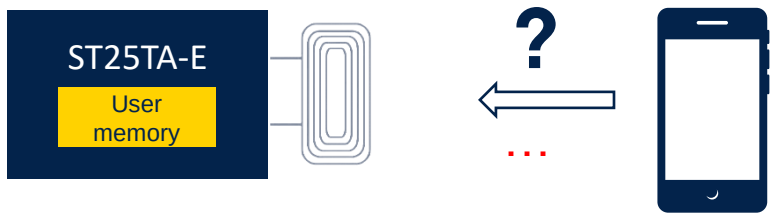
ST25TA-E Privacy

life.augmented

ST25TA-E Privacy 1/2

Kill mode : permanent deactivation of the tag

- This mode renders the ST25TA-E based tag permanently silent - persistent (no switch on/off) but stay attached to its associated item
- This mode is GDPR compliant : equivalent to the GDPR kill mode



- The user can set the ST25TA-E in this state by issuing a dedicated command protected by password. If succesful, this operation is non reversible.

ST25TA-E Privacy 2/2

Anonymous mode : privacy services

- This mode modifies the amount of identifying information – can be switched on/off after pwd authentication
- This mode is GDPR compliant : equivalent to the GDPR untraceable mode
- Once the ST25TA-E is in anonymous state, all incoming RF requests and features are handled except for :
  - The Augmented NDEF and its attributes
  - Both TruST25 (off-chip) and Edge TruST25 (on-chip) digital signatures
  - CA (Certificate Authority) file
  - Get system info and get product info commands return error code
- In such mode, the ST25TA-E uses a 4-byte UID that can be configured by the user as random or fixed value. The « real » UID is not used which ensures privacy services.

RF characteristics

NFC tuning frequency and internal tuning capacitance

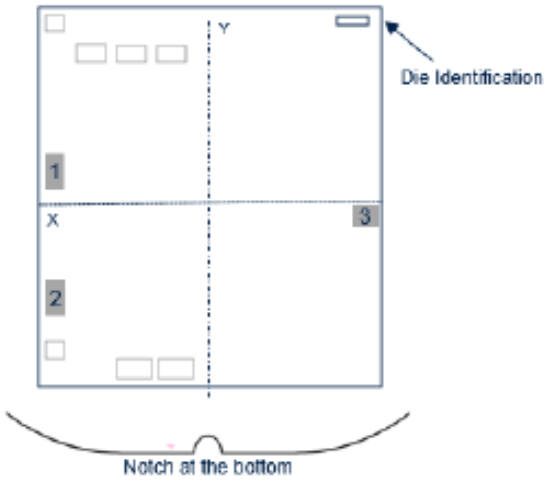
	ST25TA-E
Standard	NFC Forum type 4 tag certified - ISO/IEC 14443 Type A compliant
Main carrier frequency	13.56MHz
Data sub-carrier frequency	848 kHz
Optimal frequency tuning	13.6MHz – 14MHz
Internal capacitor (measured at 2V peak to peak)	68pF

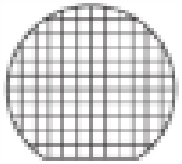
ST25TA-E delivery format

Sawn and bumped wafer

- **Sawn & Bumped wafer (production)**

  - ST25TA-E



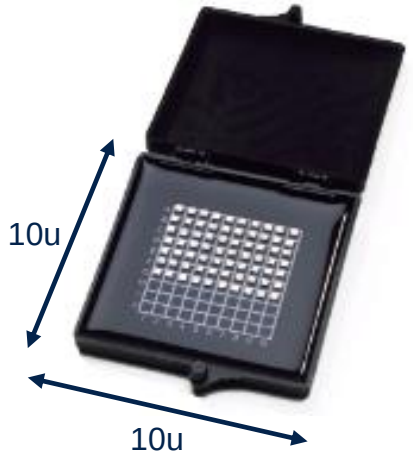


SBN14/075 *

*** : sawn and bumped inkless 12”wafer, 140µm/75um thickness**

Bump	Signal Name
1	AC0
2	AC1
3	NC

- **Gel pack (sampling)**

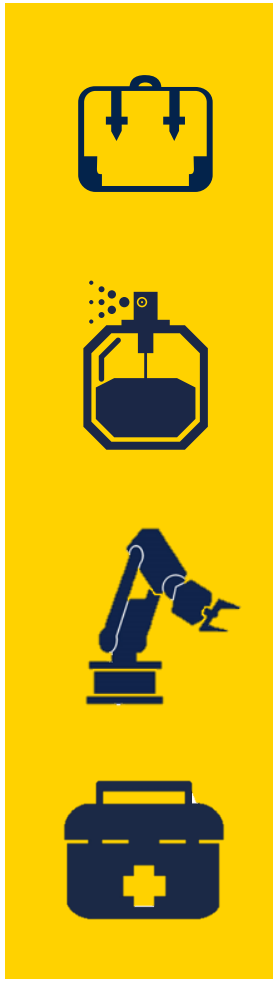


life.augmented

ST25TA-E codification

life.augmented

ST25TA-E Product part numbers

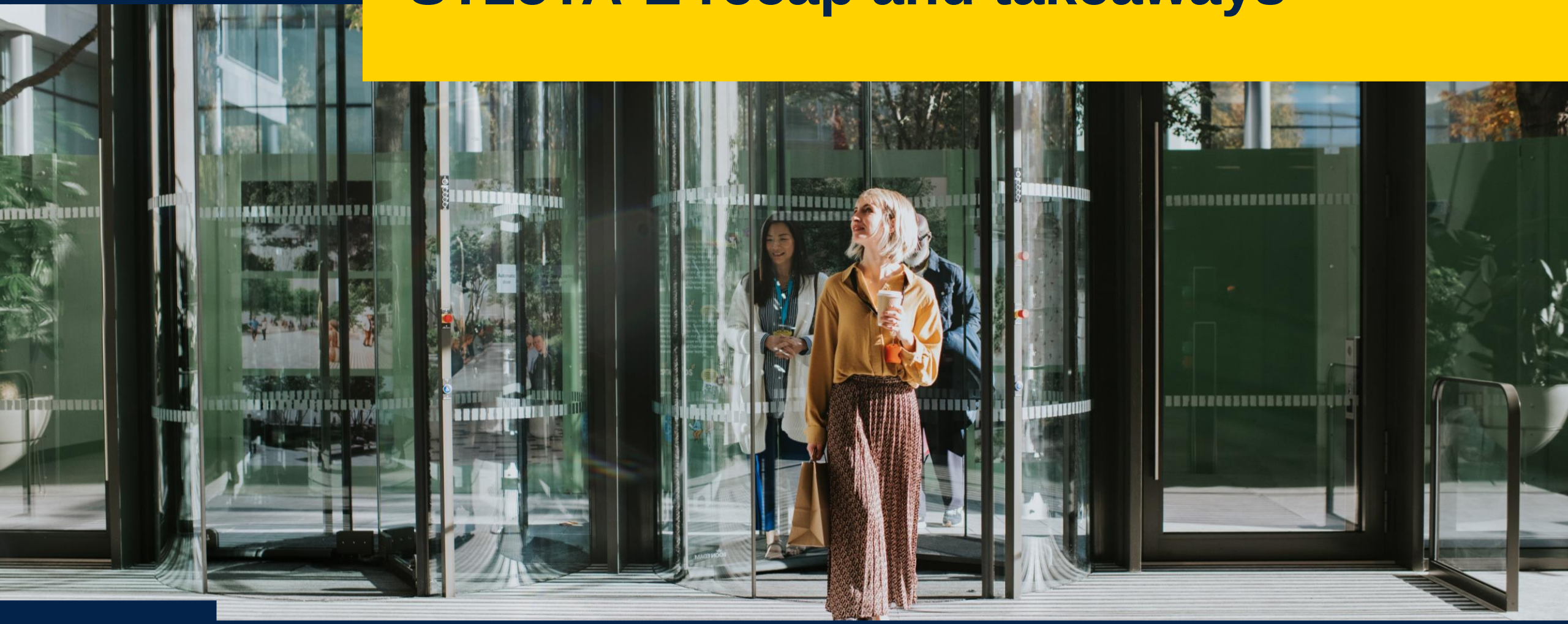


ST25TAExxx-AIy6	Package	2k-bit
NFC Type 4 Tag ISO14443	SBN14 SBN075	ST25TAExxx-AIE6 ST25TAExxx-AIF6

Xxx : customer code

life.augmented

ST25TA-E recap and takeaways



life.augmented

ST25TA-E designed for product authentication

On-chip elliptic curve digital signature algorithm (ECDSA) solution

Cloud-based application for product digitization & authentication

Unlocks new services for brands & their consumers

1 **On-chip signature** with private key

2 **In-cloud signature verification** with public key

- Secure
- Efficient
- Not predictable
- Lightweight key infrastructure

life.augmented

How to safely bridge Physical to Digital ?

QR code	Basic NFC tag	NFC Crypto tag Symmetric-based	ST25TA-E Asymmetric-based
• Not secure • Aesthetic impact • No offline data storage	• Security / robustness entry level	• Safely store secret keys on both tag and reader / application	• Highly secure and guarantee of physical asset presence (tag signature includes datas from server) • No need to safely store public key on reader / application

NFC & blockchain: A unique combination

1. Blockchain technology

Transparent I Immutable I Secure I Decentralized

2. NFC technology

Interoperable I Simple I Secure I Easy-to-integrate

Simple implementation

Strong authentication

life.augmented

ST25TA-E blockchain compatible

ST25TA-E signature format follows Blockchain standards

Signature natively supported by blockchain
Additional data treatment not needed

- Secure
- Immutable
- Transparent
- Decentralized

ST25TA-E: Benefits for everyone

Brands

- Better product traceability
- Protection against grey market
- Protection against counterfeiting
- Improved customer loyalty

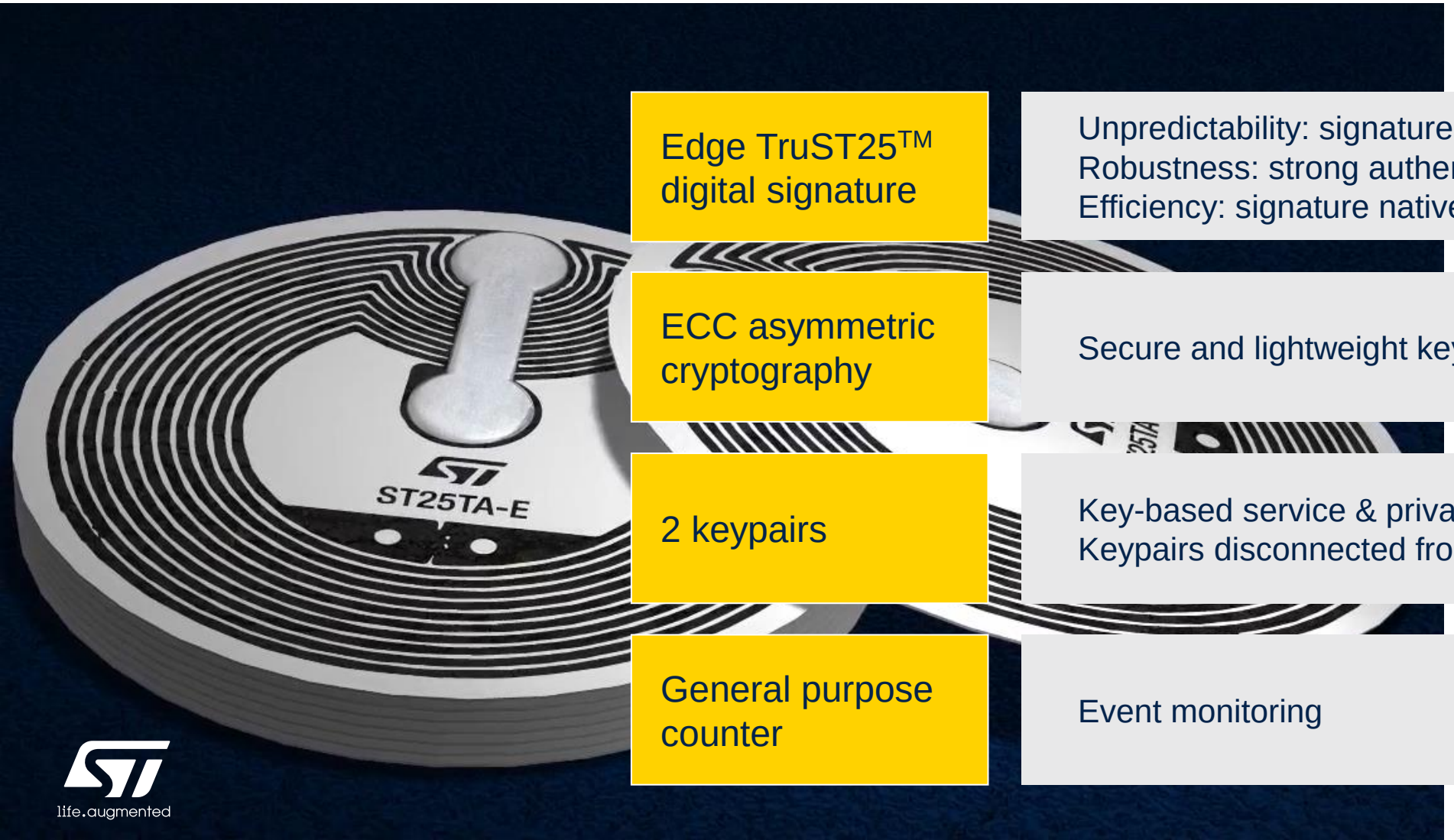
Consumers

- Protection against counterfeiting
- Product certificate for resale
- Proof of ownership
- Tailored consumer experiences

A convenient solution to easily implement
a **digital product passport** (DPP)

life.augmented

ST25TA-E added value



Edge TruST25™ digital signature	Unpredictability: signature using blockchain data Robustness: strong authentication with public key recovery Efficiency: signature natively supported by blockchain
ECC asymmetric cryptography	Secure and lightweight key infrastructure
2 keypairs	Key-based service & privacy management Keypairs disconnected from network
General purpose counter	Event monitoring

life.augmented

Thank you

life.augmented