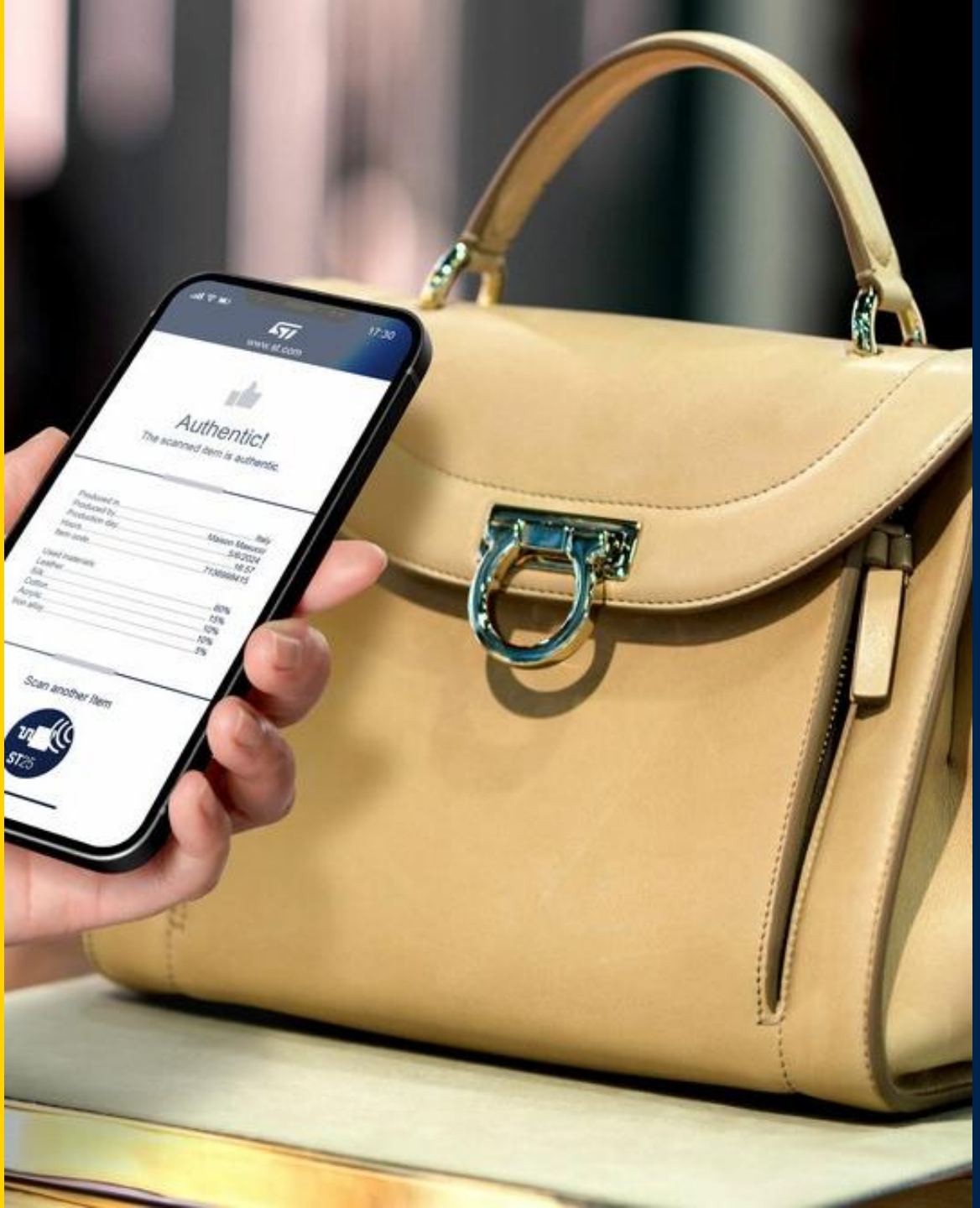


ST25TA-EB
Mint your business

ST25TA-EB main market segments

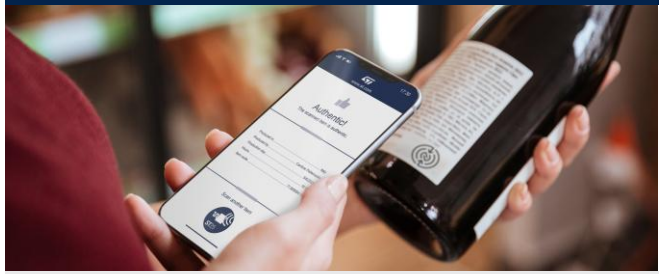
Luxury

Apparel

Jewelry / Watch

Handbag

Wines & spirits



Premium bottle

Art

Artwork

Industrial / Medical

Tool maintenance

ST25TA-EB: Benefits for everyone

Brands

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

Consumers

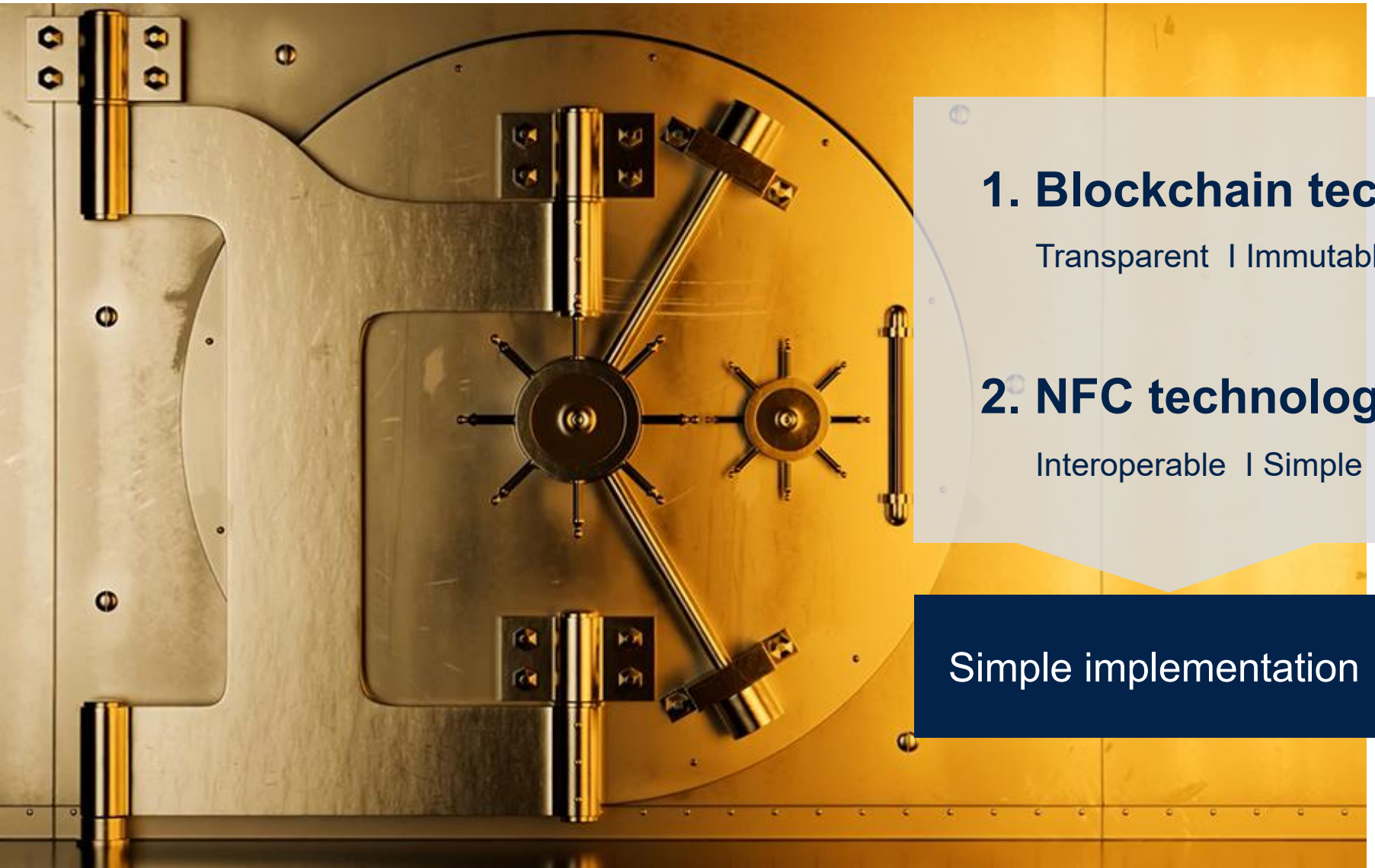
- Protection against counterfeiting
- Product certificate for resale
- Proof of ownership
- Tailored consumer experiences

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

ST25TA-EB

“Bridging
the physical and digital worlds
with the power of **NFC and blockchain**”

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

ST25TA-EB 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

ST25TA-EB blockchain compatible

ST25TA-EB signature format meets Blockchain standards

Signature natively supported by blockchain
Additional data treatment not needed

- Secure
- Immutable
- Transparent
- Decentralized

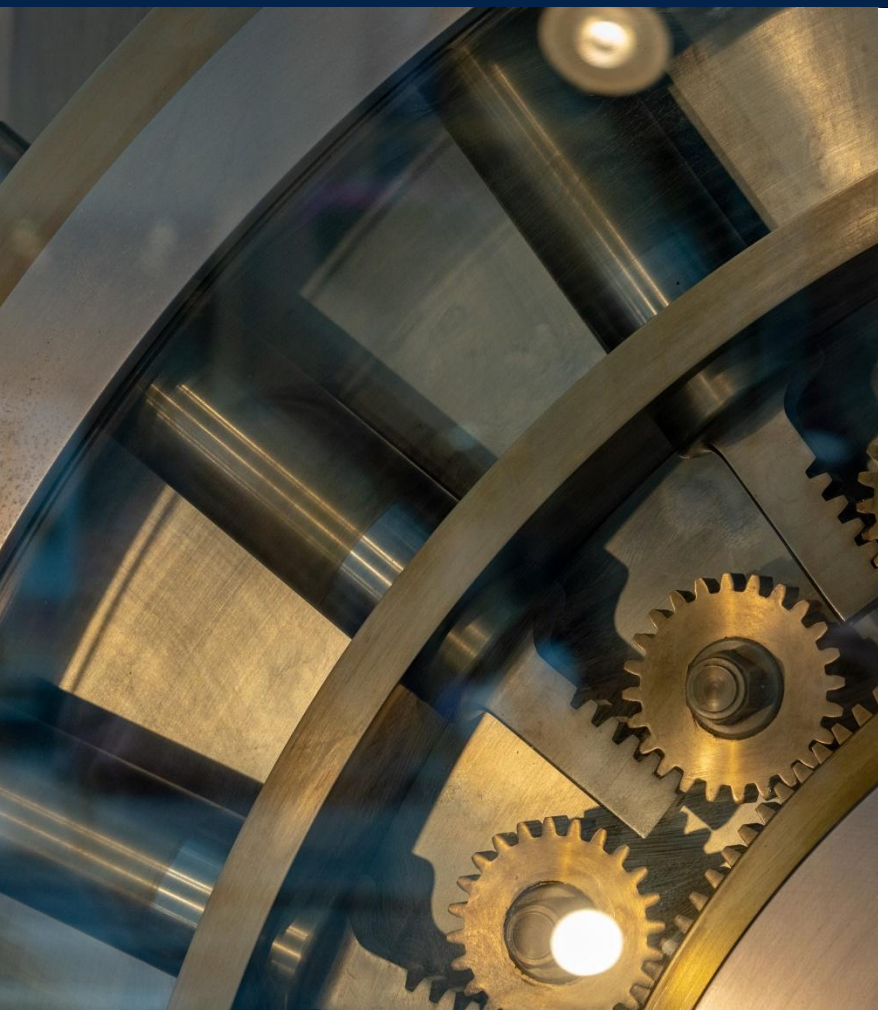
How to safely bridge the physical to digital gap?

QR code	Basic NFC tag	NFC tag with symmetric crypto	ST25TA-EB asymmetric crypto
• Not secure • Aesthetic impact • No offline data storage	• Entry-level security / robustness	• Secure storage of secret keys on both tag and reader / application	• Highly secure and guarantee of physical asset presence (tag signature includes data from server) • No need to safely store public key on reader / application

ST25TA-EB 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

ST25TA-EB architecture

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

SBN14/075
Die form, sawn and Bumped inkless 12” wafer, 140/75µm thickness

Use cases

- Brand protection, anticloning, product authentication, asset tracking

Key features

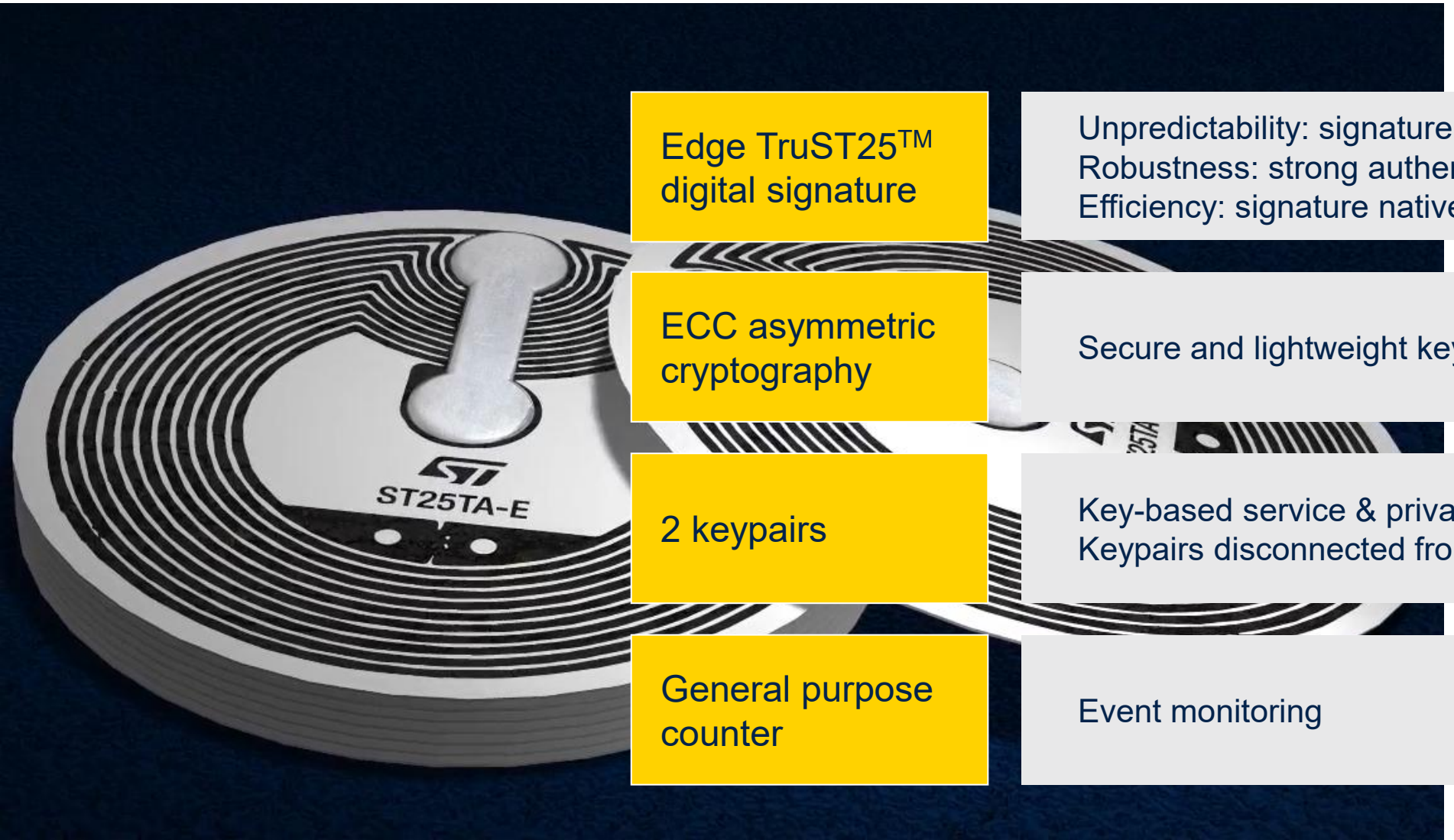
- **ISO14443-A** and **NFC Type 4**
- Short-range operations, up to **106kb/s** speed
- Data protection using password-based authentication
- **Cloning protection** thanks to Edge TruST25™ digital signature
- Configurable general-purpose counter
- **Privacy-enabled** communication modes
- Tag-related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

Key benefits

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

Explore product details here

ST25TA-EB added value

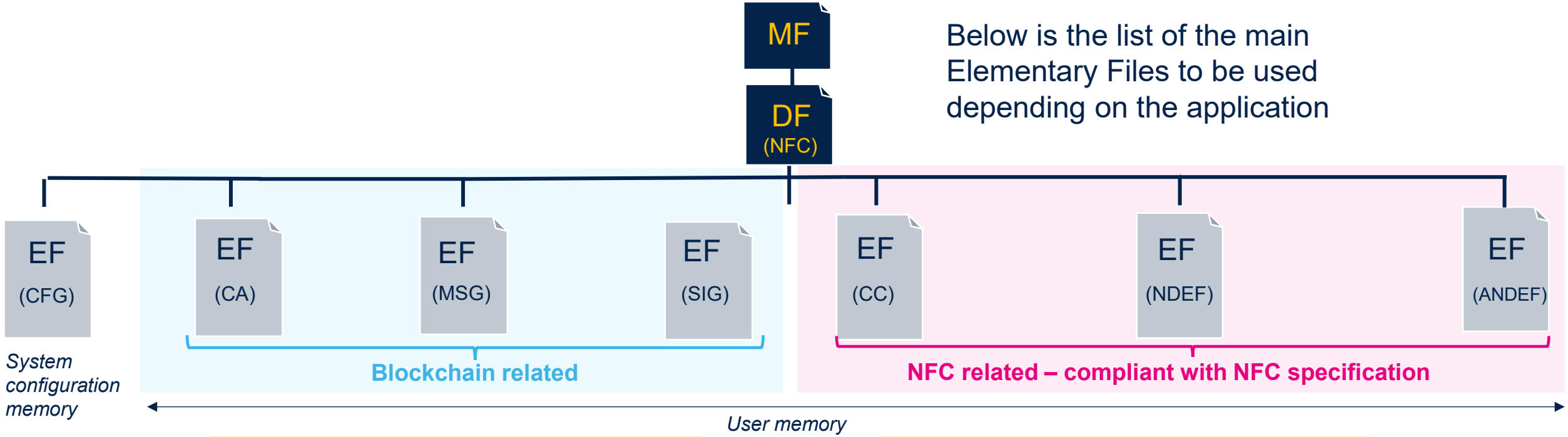


Edge TruST25™ digital signature	Unpredictability: signature using blockchain data Robustness: strong authentication with public key recovery Efficiency: signature natively supported by blockchain
ECC asymmetric cryptography	Secure and lightweight key infrastructure
2 keypairs	Key-based service & privacy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

Technical insights
ST25TA-EB Memory mapping

ST25TA-EB Memory organization

The ST25TA-EB 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

Technical insights
ST25TA-EB file protection

ST25TA-EB permanent lock file protection

- Each elementary file can have individual read and/or write access permissions to **prevent unauthorized reading of a file or writing to a file.**
- The permanent lock file mechanism **permanently changes the file's memory content so that it can only 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.
- 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

ST25TA-EB password protection

- The reversible lock file protection mechanism is based on password authentication. It can restrict access to certain ST25TA-EB features and commands, and prevent read and/or write access to data stored in each elementary file of the user or system configuration memory.
- Each ST25TA-EB password is 64-bit length and comes with a default value
- ST25TA-EB devices can protect passwords against brute-force attacks by limiting the number of failed login attempts.

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

Technical insights
ST25TA-EB Augmented NDEF

ST25TA-EB Augmented NDEF

Advanced NDEF message services

- Augmented NDEF lets the tag provide dynamic, context-aware content automatically, without manually updating the stored message in the memory
- 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

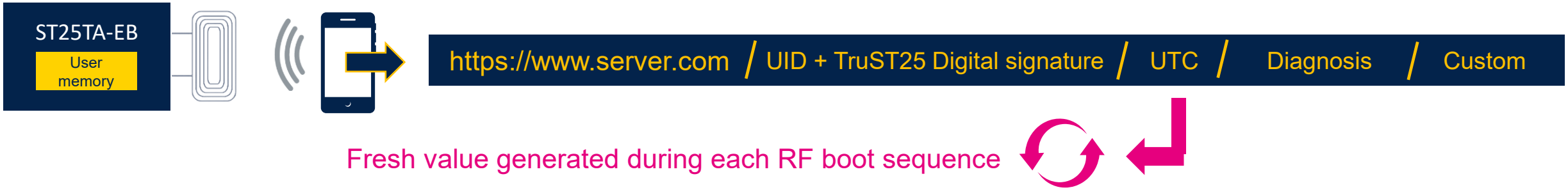
Automatically added at each “tap”

Each attribute can be enabled/disabled

ST25TA-EB Unique Tap Code (UTC)

Unique code generator

- The UTC is a 4-digit 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 an anti-tearing mechanism that ensures counter consistency, even in the event of an electrical problem during incrementing.
- The UTC can be configured, activated, and read natively.



Technical insights
ST25TA-EB TruST25™ label

TruST25™ Label

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

TruST25™ umbrella

Non secure ST25T

Entry-level TruST25™ services

What	*Why*
TruST25™ digital signature (off-chip)	ST tag IC authentication
TruST25™ password-related authentication	User data protection

Secure ST25T (i.e. ST25TA-EB)

Premium TruST25™ services

What	*Why*
Edge TruST25™ digital signature (on-chip)	Physical asset authentication
TruST25™ password-related authentication	User data protection

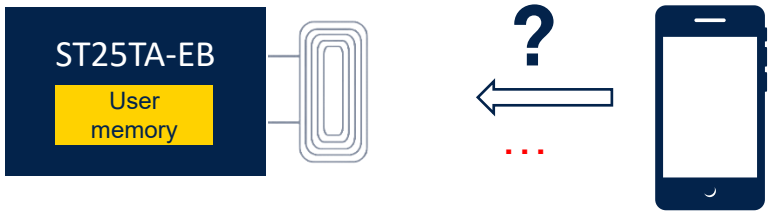
Please contact your STMicroelectronics sales office to get more information about the TruST25™ digital signature features

Technical insights
ST25TA-EB Privacy

ST25TA-EB Privacy 1/2

Kill mode: permanent deactivation of the tag

- Makes the ST25TA-EB tag permanently silent and persistent (with no on/off switching), while keeping it attached to its associated item.
- GDPR compliant: equivalent to the GDPR kill mode



- The user can set the ST25TA-EB to this mode by issuing a dedicated command protected by a password. If successful, the operation cannot be reversed.

ST25TA-EB Privacy 2/2

Anonymous mode: privacy services

- Modifies the amount of identifying information – can be switched on/off after password authentication
- GDPR compliant: equivalent to the GDPR untraceable mode
- Once the ST25TA-EB 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 this mode, the ST25TA-EB uses a 4-byte UID that the user can configure as either random or fixed. The “real” UID is not used, which helps ensure privacy.

RF characteristics

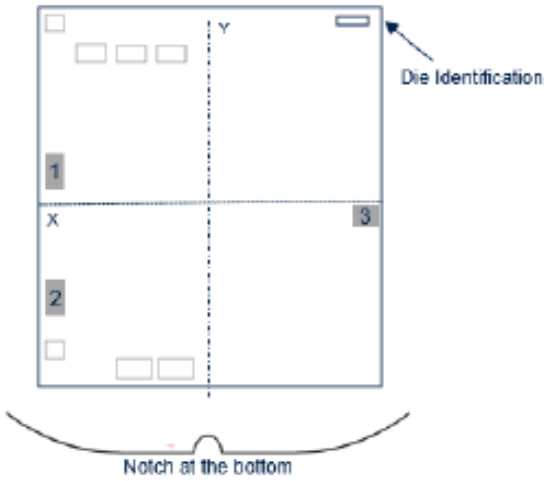
NFC tuning frequency and internal tuning capacitance

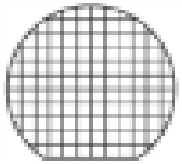
	ST25TA-EB
Standard	NFC Forum type 4 tag certified - ISO/IEC 14443 Type A compliant
Main carrier frequency	13.56MHz
Data sub-carrier frequency	848 kHz
Optimal frequency tuning	13.6 MHz – 14 MHz
Internal capacitor (measured at 2 V peak to peak)	68 pF

ST25TA-EB delivery format

Sawn and bumped wafer

- **Sawn & bumped wafer (production)**
  - ST25TA-EB



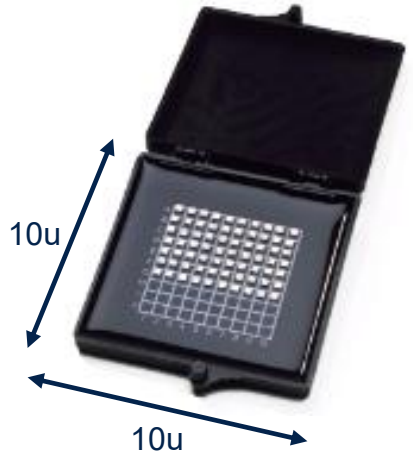


SBN14/075 *

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

Bump	Signal Name
1	AC0
2	AC1
3	NC

- **Gel pack (sampling)**



Technical insights
ST25TA-EB codification

ST25TA-EB
Product part numbers

ST25TAEB	Package	Personalization	Codification
NFC Type 4 Tag ISO14443, 2k-bit	SBN14	Internal* External**	ST25TAEBxxx-AIE6 ST25TAEBxxx-AOE6

xxx : customer code

*: certificates and parameters configured by ST (HSM)

**: certificates and parameters configurable by inlay makers / partners

Our technology starts with You

st.com/luxury-ST25TAEB