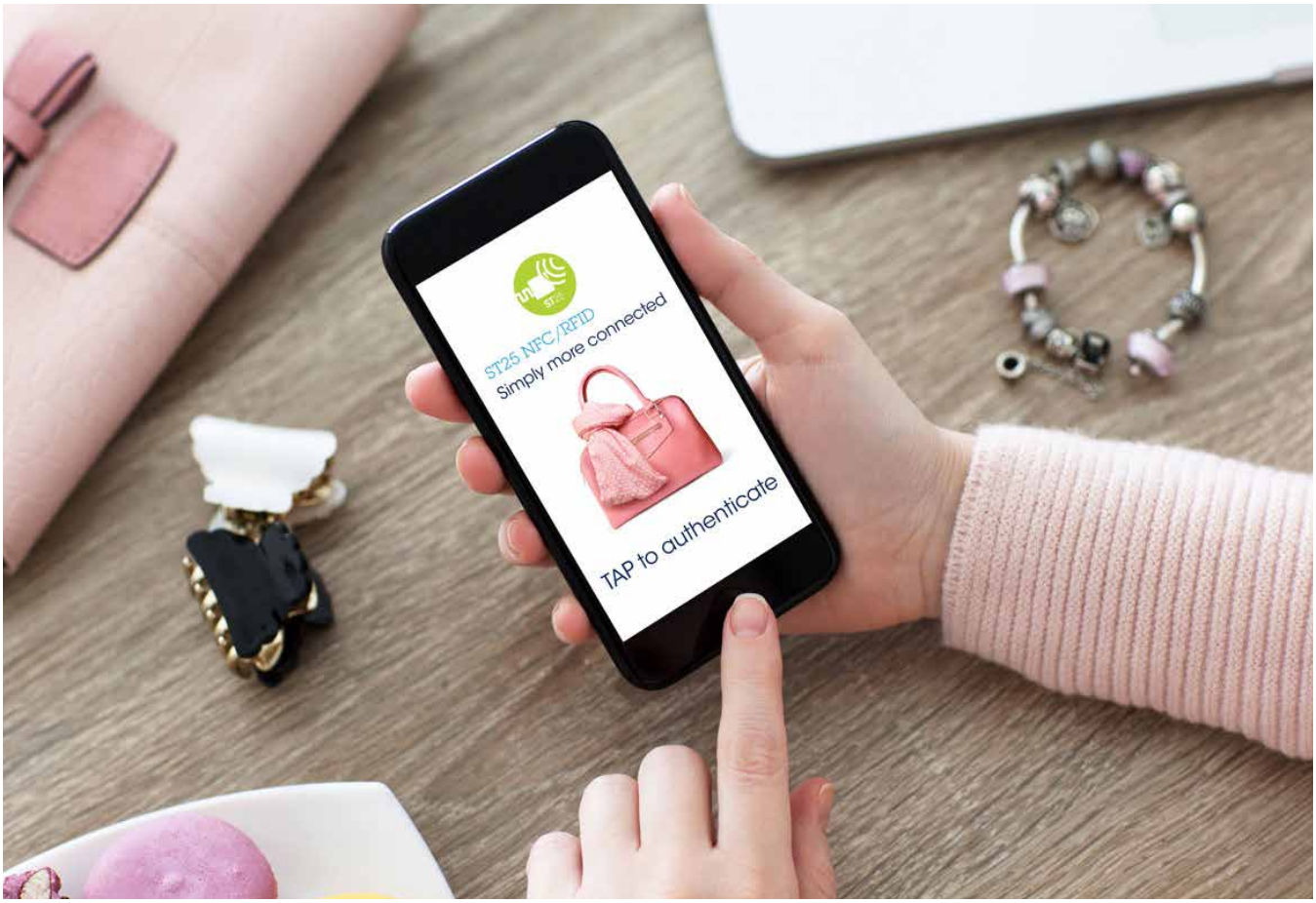
TruST25™ Digital signature
Authenticity with ST25 NFC/RFID tags

life.augmented

Discover how NFC/RFID tags with an embedded digital signature eliminate the risk of counterfeit and gray market goods. Thanks to this cryptographic solution and a secure manufacturing environment, it is now possible to guarantee the integrity of products and authenticate their origin.



HOW CAN I RELIABLY AUTHENTICATE MY PRODUCTS?

Supply chains inevitably face the risk of gray market distribution channels and counterfeit goods. The use of RFID/NFC tags is a widely used solution to counter these threats.

Before it reaches the end-customer, an RFID/NFC tag undergoes a rather long manufacturing process: from the silicon manufacturer to the inlay or raw material maker, then to the system integrator and finally to the end-product assembler. Each of these steps involve different companies, with all their associated logistics.

Counterfeiting may come up in each of these phases. And because business requires trust, a commercial delivery requires guarantees. How can you prove that a tag embeds the expected silicon with the expected quality? How can you prove that a tag is authentic? How can you prove that a product is legitimate?

USING RFID/NFC TAGS TO FIGHT RETAIL FRAUD AND COUNTERFEITING

Each step of the supply chain represents a potential point of entry for counterfeit and gray market goods.

From factory... ... to consumer

As each tag features a Unique Identifier (UID), the use of RFID/NFC technology is an intrinsically trustworthy means of ensuring the correct identification of key elements. This UID can easily be traced back to the silicon manufacturer and all along the supply chain.

UIDs are assigned to manufacturers by an ISO/IEC committee. In compliance with RFID/NFC specifications, this UID is readable by any RFID reader or NFC-enabled phone.

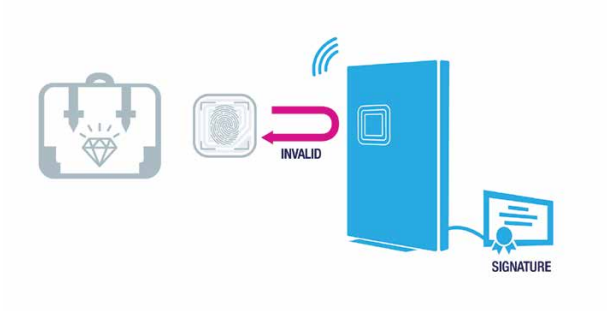
Moreover, UIDs can be used by customers to check if the product they bought is genuine.

This clearly requires that the UID be issued by the legitimate silicon manufacturer. As an example, if a silicon foundry manufactures RFID/NFC tags using UIDs assigned to another manufacturer, it opens the door to counterfeiters. Counterfeited tags and counterfeited end-products may enter the market and take a share of the business.

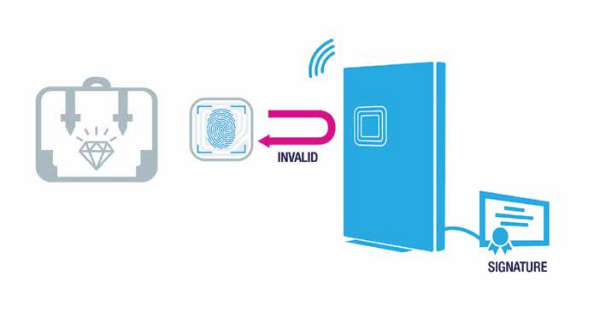
Reading the UID is not enough to know who really manufactured the tag.

USING DIGITAL SIGNATURES TO RELIABLY GUARANTEE AUTHENTICITY

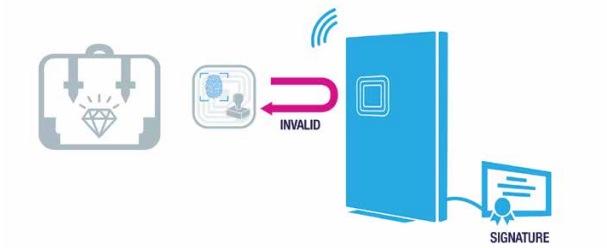
Cryptography provides a solution to easily and reliably verify the authenticity of the origin of an RFID/NFC tag: the digital signature.
A digital signature is an intrinsically secure type of electronic signature that can be processed to guarantee the integrity of the signed content and authenticate its origin (signer).
There are four ways in which an RFID/NFC tag can be counterfeit and where digital signature will prove the origin of the tag:



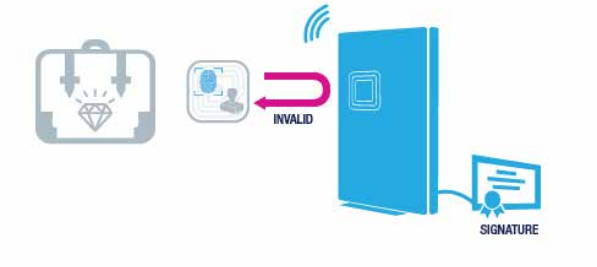
The tag features a UID not assigned to the legitimate manufacturer.
Simply reading the UID will discover the substitution.



The tag features a UID assigned to the legitimate manufacturer, but does not embed a digital signature.
When the digital signature is requested, the tag will not answer, thus revealing the counterfeit.



The tag features a UID assigned to the legitimate manufacturer and embeds a digital signature, but with a digital signature not issued by the legitimate manufacturer.
By verifying the digital signature, the reader can reliably determine if the UID was really issued by the legitimate manufacturer.

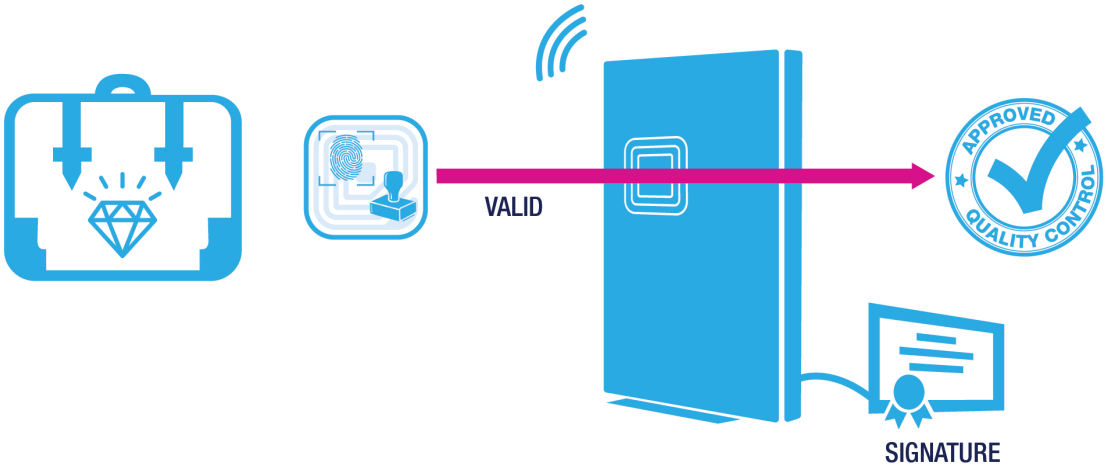


The tag features a UID assigned to the legitimate manufacturer and embeds a copy of a digital signature issued by the legitimate manufacturer.
By verifying the uniqueness of the UID, the reader can readily determine that the UID is a duplicate – hence the tag is a fake.

By using a UID with a digital signature, an inlay maker can sell its inlays with a guarantee that the embedded silicon chips (tags) are genuine. Furthermore, the inlay maker may also use the digital signature to provide a means for their customers to readily verify the authenticity of the inlay.
This leads to an increase of trust, and therefore of business.

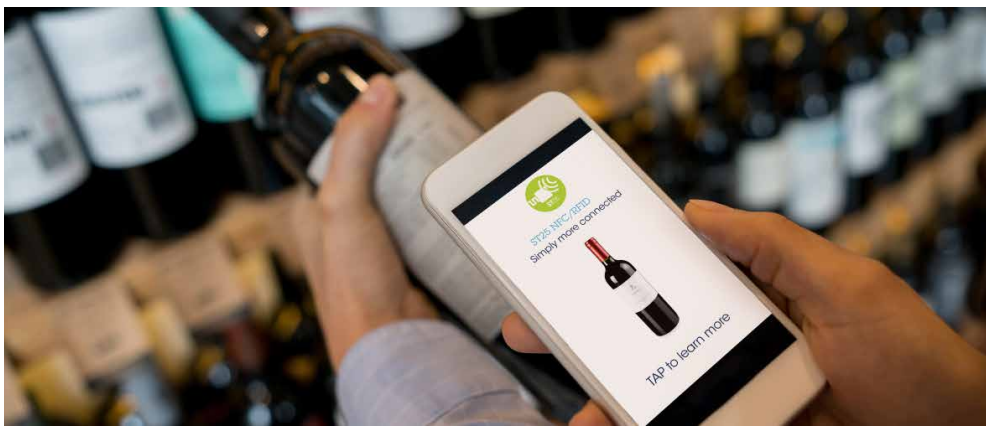
GETTING STARTED WITH TRUST25 DIGITAL SIGNATURE

The TruST25™ digital signature by STMicroelectronics, a recognized world leader in semiconductor solutions, is manufactured in compliance with the highest security standards. ST's industrialization processes and tools are used to store private encryption keys and generate signatures using a certified hardware security module (HSM) in a secure room to guarantee the uniqueness of an NFC/RFID tag's digital signature.
The use of TruST25™ digital signatures makes it possible to reliably catch counterfeit tags or clones, increasing trust all along the supply chain.



The TruST25™ digital signature is an enabler for confidence throughout the entire supply chain, providing an intrinsically secure means of product identification from silicon manufacturer to end customer.
In addition to the supply chain, TruST25™ digital signatures can also be used to track objects as they move through their journey to help streamline delivery management systems.
RFID/NFC tags can also be read using smartphones equipped with NFC readers. This enables the development of new services for improving user engagement by retailers and brands, as well for increasing revenue. Here too, the use of TruST25™ digital signatures will ensure a higher of level of trust in the user experience.

Developers and companies looking to protect supply chains or bring trust to final goods' journey can find more information about ST's products and solutions on **www.st.com/st25**



For more information on how to verify the authenticity of an NFC/RFID tag's digital signature, refer to the technical article TA0358 on st.com.

PRODUCT PORTFOLIO

Part number	RF Interface	NFC Forum certtification	Memory size	Data protection	Counter	Special features	Package	Wired interlace
ST25T								
ST25TA512B	ISO14443 Type A NFC Forum Type 4	YES	512-bit	128-bit password	20-bit	TruST25® Digital signature	SBN12 (*)	NO
ST25TA02KB	ISO14443 Type A NFC Forum Type 4	YES	2-Kbit	128-bit password	20-bit	TruST25® Digital signature	SBN12 (*)	NO
ST25TA02KB-P	ISO14443 Type A NFC Forum Type 4	YES	2-Kbit	128-bit password	20-bit	TruST25® Digital signature	UFDFPN5	Yes (CMOS positive GPO)
ST25TA02KB-D	ISO14443 Type A NFC Forum Type 4	YES	2-Kbit	128-bit password	20-bit	TruST25® Digital signature	UFDFPN5	YES (Open Drain GPO)
ST25TV512	ISO15693 NFC Forum Type 5	YES	512-bit	32/64-bit encrypted password	16-bit	TruST25® Digital signature	UFDFPN5, SBN075 and SBN12 (*)	NO
ST25TV02K	ISO15693 NFC Forum Type 5	YES	2-Kbit	32/64-bit encrypted password	16-bit	TruST25® Digital signature	UFDFPN5, SBN075 and SBN12 (*)	NO
ST25TV02K-AD	ISO15693 NFC Forum Type 5	YES	2-Kbit	32/64-bit encrypted password	16-bit	Tamper detect pin/ TruST25® Digital signature	UFDFPN5, SBN075 and SBN12 (*)	NO
ST25D								
ST25DV02K-W1	ISO15693 NFC Forum Type 5	YES	2-Kbit	32/64-bit password	NA	TruST25® Digital signature	SO8, TSSOP8	1 PWM
ST25DV02K-W2	ISO15693 NFC Forum Type 5	YES	2-Kbit	32/64-bit password	NA	TruST25® Digital signature	SO8, TSSOP8	2 PWM

life.augmented

Order code: BRWPDIGSIGN0419

For more information on ST products and solutions, visit www.st.com