

WHY A TRUSTED TAP IS MORE THAN A LINK

BrandGuard™ connects a protected physical product to a secure NFC identity and an online verification decision. It gives the customer meaningful evidence about the current tap - not merely a destination that can be copied.



01

ENGINEERED FOR THE PRODUCT

The NFC form is selected around the real object and its operating conditions.

02

PROTECTED DIGITAL EVIDENCE

A secure credential produces authenticated data for the current interaction.

03

A MEANINGFUL RESULT

The verification service evaluates the evidence before returning the approved response.

STATIC ACCESS OR VERIFIED INTERACTION

A copied link can look genuine.

A QR code or basic NFC tag can open the correct website. That alone does not establish which physical object the customer has touched.

STATIC ACCESS

The destination is visible

A URL, QR code or public NFC record tells the phone where to go. The same visible data may be copied onto another object and still open the same page.

BRANDGUARD VERIFICATION

The current tap is assessed

A security-capable NFC chip produces authenticated data for the interaction. The verification service evaluates that evidence before returning the current result.

THE THREE QUESTIONS BEHIND A TRUSTED TAP

01

Expected identity

The service checks evidence tied to the credential assigned to the intended product record.

02

Consistent evidence

Authentication and read-counter context help evaluate whether the evidence is valid, stale, repeated or otherwise inconsistent.

03

Product connection

The label, seal, cable, badge or durable tag is engineered to remain attached or show evidence of removal or opening as the application requires.

THE IMPORTANT DISTINCTION

The webpage is the destination. Trust comes from validated cryptographic evidence, the expected product identity and the physical way that identity is integrated with the product.

BROWSER-BASED VERIFICATION

One customer action. Five connected checks.

The customer simply taps with a compatible NFC-enabled phone. The secure evidence and verification decision are handled behind the browser experience.

01

Tap the protected product

The phone reads the BrandGuard NFC element. A dedicated consumer app is not required for the standard browser flow.

02

Create authenticated evidence

The secure chip uses its protected credential and Secure Dynamic Messaging (SDM) to generate a Secure Unique NFC (SUN) authentication message for the current read.

03

Send the verification request

The phone opens a normal web request and carries the dynamic data to the verification service.

04

Evaluate the current interaction

The service checks the authentication code, expected identity and relevant read or tamper context for the approved project.

05

Return the approved result

The customer receives the result for this tap and can continue to product information, service or brand-approved content.

WHY THE BROWSER IS NOT THE SECURITY DECISION

The browser carries the request and displays the response. The verification service decides whether the evidence behind the tap is valid for the expected product and project rules.

PUBLICLY DOCUMENTED CAPABILITIES

What protects the digital evidence.

BrandGuard solutions may use NXP NTAG® 424 DNA and, where specified, NTAG® 424 DNA TagTamper. The capabilities below are public; their value comes from correct product integration and verification.

CAPABILITY	PUBLIC FUNCTION	WHAT IT MEANS FOR THE CUSTOMER
AES-128	A widely reviewed cryptographic foundation used to protect authentication operations.	The decision can rely on protected evidence rather than visible text alone.
AES-CMAC	A message authentication code that can be checked against the expected credential.	The service can detect protected authentication data that is invalid for the expected credential or has been altered.
Individual credential	Each approved NFC identity is associated with its intended item record.	Copying public data does not reproduce the protected credential needed for a new valid message.
SDM / SUN	Read-related authenticated data is carried through a standard NFC web interaction.	A secure browser-based customer experience is possible without a dedicated app.
Read-counter context	Sequence information can be evaluated across relevant reads; it is not a timestamp.	Compared with verification history, it can help flag replayed, out-of-sequence or otherwise inconsistent evidence.
TagTamper option	With the TagTamper variant and a qualified loop, the authenticated data can include current and once-opened state.	The result can include evidence of opening; it does not identify the cause or guarantee the product condition.

WHAT COPYING STILL FAILS TO REPRODUCE

COPY A URL OR PUBLIC MEMORY

The destination may open, but the copy cannot create a new valid message from the expected protected credential.

REPLAY AN EARLIER REQUEST

Previously valid data may be identified as stale, repeated or inconsistent through counter context and verification history.

MOVE A GENUINE TAG

Cryptography alone cannot prevent physical transfer. A destructible, closure-crossing, cable or qualified tamper construction helps mitigate that risk.

BEYOND THE CHIP

A secure chip is the foundation. BrandGuard makes it product-ready.

The customer receives a qualified system connecting the physical product, its secure identity, controlled production and the verification experience.

01

Product engineering

The NFC form, antenna, materials and attachment method are selected around the real object. Read performance and intended removal or opening behaviour are confirmed on the finished product.

02

Controlled production

Each encoded identity is associated with the intended product record. Secure encoding and item-level traceability are brought into a controlled, repeatable production workflow.

03

Verification and support

The online checks and approved customer result are configured for the project, with support for production transition, exceptions and the credential lifecycle.

PHYSICAL FORMS SELECTED AROUND THE APPLICATION



DESTRUCTIBLE LABEL



CLOSURE SEAL



CABLE SEAL



GARMENT BADGE



DURABLE TAG

WHY THIS MATTERS

A secure chip cannot compensate for poor installed read performance, unsuitable attachment or an uncontrolled identity process. BrandGuard develops these elements as one qualified system around the real product.

FROM SECURE PRODUCT FORM TO COMPLETE VERIFICATION

Choose the delivery scope that fits the project.

BrandGuard can supply an engineered physical form, add controlled secure encoding, or deliver the physical product protection and online verification as one connected solution.

A**PHYSICAL PROTECTION**

An engineered NFC label, seal, badge, cable seal or durable tag selected and qualified around the application.

B**PROTECTION + SECURE ENCODING**

The qualified physical form plus secure item-level encoding for use with an approved customer verification environment.

C**INTEGRATED BRANDGUARD PROTECTION**

Physical protection, secure NFC identity and BrandGuard online verification delivered as one connected solution.

WHERE BRANDGUARD CAN BE USED

- Product authentication and premium packaging
- Closure monitoring and one-time seals
- Garments, footwear and reusable objects
- Equipment cases and logistics applications
- Digital product passports and after-sales experiences

THE ACCURATE SECURITY CLAIM

No single technology makes a product impossible to counterfeit. BrandGuard makes copied static content insufficient and provides stronger evidence for assessing the tap. With an appropriate physical construction, it can also make transfer or reuse more difficult. Final performance depends on the approved product integration, operating environment and verification scope.

Discuss the product, environment and verification objective.

We can define the physical form, secure identity and verification scope as one project.

BRAND GUARD™

sales@accuz.com

brandguard.co

ACCUZ®