A PRIMER ON PRODUCT AUTHENTICATION

How do you prove a physical product isn't a counterfeit?

It's a question every brand, regulator, and supply chain has to answer. There are many solutions, each with their own applications and caveats. This is a look at what authentication actually means and how the field approaches it.

BY JOHN WOLFE · CEO, NOVAVERA

THE SCALE

Counterfeit trade hit $467 billion in 2021. By 2030 it could reach $1.79 trillion.

$467B
TRADE IN FAKES, 2021 (OECD)

2.3%
OF TOTAL GLOBAL IMPORTS (OECD)

$1.79T
2030 INDUSTRY PROJECTION (CORSEARCH)

The OECD and EUIPO documented $467 billion in cross-border counterfeit goods in their most recent global survey. Industry analysts project that figure to more than triple by the end of the decade. The technologies built to stop counterfeiting now sit at the center of supply chain, regulatory, and brand strategy decisions.

SOURCES: OECD/EUIPO MAPPING GLOBAL TRADE IN FAKES 2025; CORSEARCH 2024 PROJECTION

THE TERM

Product authentication is the process of verifying that a physical product is genuine.

It's a yes-or-no verification problem about a specific physical object. Did this come from the legitimate source? Is the material in front of you the material it claims to be?

> *ISO 12931 frames authentication as the verification of a material good's claim of authenticity. It is the international standard for authentication solutions.*

Within that standard, authentication features fall into three families: **overt**, **covert**, and **forensic**. They differ in who can verify them, what tool is needed, and how long verification takes.

SOURCES: ISO 12931:2012; ISO 22383:2020

FAMILY 01 · OVERT

Visible features. The ones you can see.

Authentication elements detectable by human senses without any tool. Anyone can verify them in seconds, with no equipment.

Holograms · Color-shifting ink · Watermarks · Microprinting · Tamper-evident seals

STRENGTHS

+ Anyone can verify without equipment
+ Low cost to deploy at scale
+ Effective consumer-level deterrent

LIMITATIONS

– Visible features tell counterfeiters what to copy
– "Good enough" imitations are easy to produce
– Tend to drift toward marketing element over time

SOURCES: ISO 12931:2012; WIPO MAGAZINE, "THE ROLE OF AUTHENTICATION TECHNOLOGIES IN COMBATING COUNTERFEITING"

FAMILY 02 · COVERT

Hidden features. Visible only with a tool.

Authentication elements hidden from human senses until a specific tool reveals them. Often embedded into the product material or packaging substrate during manufacturing.

UV / IR inks · Chemical taggants · Embedded fluorophores · Magnetic threads · Molecular markers

STRENGTHS

+ Counterfeiters cannot copy what they cannot see
+ Can be embedded inside the material itself
+ Works as a layered defense with overt features

LIMITATIONS

– Requires verification equipment in the field or lab
– Higher initial integration and tooling cost
– Limited consumer-level utility

SOURCES: ISO 12931:2012; WIPO MAGAZINE, "THE ROLE OF AUTHENTICATION TECHNOLOGIES IN COMBATING COUNTERFEITING"

FAMILY 03 · FORENSIC

Lab-grade features. Verified only by experts.

The deepest layer. Authentication elements verified only by skilled experts using laboratory equipment. Used to resolve disputes when other layers are in question.

DNA taggants · Isotope ratios · Spectroscopic signatures · Chemical fingerprints · Microscopic markers

STRENGTHS

+ Strongest verifiable evidence, legal-grade
+ Definitive resolution of authenticity disputes
+ Hardest category for counterfeiters to replicate

LIMITATIONS

– Slow: hours to days, not seconds
– Expensive per verification
– Not viable for routine high-volume checks

SOURCES: ISO 12931:2012; WIPO MAGAZINE, "THE ROLE OF AUTHENTICATION TECHNOLOGIES IN COMBATING COUNTERFEITING"

IN PRACTICE

The strongest systems layer multiple families.

No single category answers every threat. Real-world authentication usually pulls from two or three families at once: overt for consumer-level reassurance, covert for inspector-level verification, forensic for legal disputes.

BANKNOTES	Overt + Covert + Forensic
PHARMA PACKAGING	Overt + Covert
INDUSTRIAL PARTS	Covert + Forensic

> *ISO 12931 establishes that combining multiple authentication elements raises both the cost of attack and the security level of the solution.*

SOURCE: ISO 12931:2012, MULTI-ELEMENT APPROACH

AT A GLANCE

Three approaches, side by side.

	OVERT	COVERT	FORENSIC
VISIBLE TO EYE	Yes	No	No
TOOL TO VERIFY	None	Handheld reader	Laboratory
TIME TO VERIFY	Seconds	Seconds	Hours to days
VERIFIER	Anyone	Inspector	Lab expert
RESISTANCE TO COPYING*	Low	High	Very high

*PRACTITIONER CONSENSUS ON RELATIVE ATTACK RESISTANCE. ISO 22383:2020 ESTABLISHES THE FRAMEWORK, NOT THE RATINGS.
SOURCES: ISO 12931:2012; ISO 22383:2020; WIPO MAGAZINE, 2024

THREE THINGS TO TAKE FROM THIS

What this primer tried to make visible.

01 Authentication is a yes-or-no question about a specific physical object. Answering it requires a feature in or on the product itself: a marker, a signature, an embedded element that can't be faked at scale.

02 Three broad families of solutions exist (overt, covert, forensic). Each has real strengths and real limitations. None is universally best.

03 The strongest systems combine multiple families. Banknotes use all three. The right question for a buyer isn't "which technology should I pick." It's "which combination fits this risk."

REFERENCES ISO 12931:2012 · ISO 22383:2020 · OECD/EUIPO, Mapping Global Trade in Fakes 2025 · Corsearch, May 2024 · WIPO Magazine, 2024 · Grand View Research, 2025

John Wolfe is CEO of NovaVera, which builds authentication infrastructure for high-stakes products: currency, pharmaceuticals, luxury goods, and industrial materials. Field Notes is a series for practitioners. Follow NovaVera for the next briefing.