

Security and Authentication Features for Printed Products, Packaging and Documents

Material-enabled overt, covert and forensic features that can support, but do not establish, regulatory traceability

Dr. Juan Seguro, founder and Scientific Director · 3Dresyns by Resyner Technologies S.L. · General Etxague 15B, 20003 Donostia / San Sebastián, Gipuzkoa, Spain · info@3dresyns.com · www.3Dresyns.com

Highlights

- Thermochromic, photochromic, fluorescent and infrared features are tools within a security architecture.
- Effectiveness requires threat modelling, controlled verification and resistance-to-copy testing.
- A material feature may complement a UDI carrier but does not create UDI compliance.
- Regulation (EU) 2019/1020 does not generally require products to contain authentication materials.
- Adding a marker changes the formulation and can alter optical, mechanical, chemical and biological evidence.

Abstract

Material-enabled security features can support authentication of printed products, packaging and documents, but their value depends on the threat model, secrecy, verification infrastructure and resistance to copying.

Regulation (EU) 2017/745 establishes Unique Device Identification requirements for medical devices. A printed feature may complement a UDI carrier or anti-counterfeit system, but it does not itself create UDI compliance. Regulation (EU) 2019/1020 is a market-surveillance framework and is not a general mandate for authentication materials.

Every marker is treated as a formulation change. Performance and any final-product chemical, biological or regulatory implications require system-specific evidence.

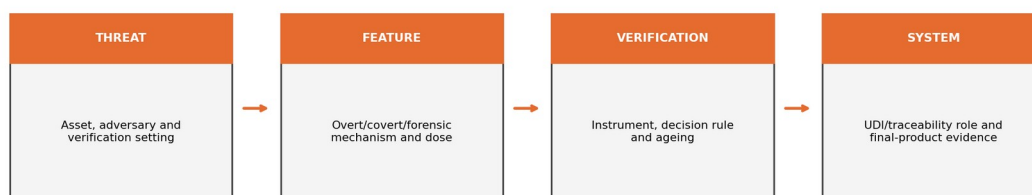
Keywords authentication · anti-counterfeit · UDI · traceability · security feature · threat model

Source use. Product evidence is controlled in [1]; legal scope in [2–3]; authentication and identification methods in [4–5]; material context in [6].

1. Threat-led feature selection

Overt, covert and forensic features address different attack and verification scenarios. Selection begins with the adversary, protected asset, inspection setting, false-positive/false-negative risk and lifecycle.

- Define who verifies the feature and with what instrument.
- Test durability after ageing and handling.
- Avoid unsupported global counterfeit-loss figures.



Release requires traceable evidence at every gate; a catalogue label cannot bypass the chain.

Figure 1. WP-21 evidence gates from controlled material description to final acceptance.

2. UDI, serialization and authentication

UDI carrier, serialization, track-and-trace and material authentication are related but distinct systems. The complete identifier, carrier, database and manufacturer obligations determine UDI compliance.

- Do not equate a security resin with compliance.
- Validate readability and data integrity.
- Separate regulatory traceability from anti-counterfeit strength.

3. Formulation and final-product boundary

A marker can change cure, colour, mechanics, extractables and biological response. The final formulation and finished product require the applicable evidence and change control.

4. Minimum controlled evidence before release

Control field	Required record	Release interpretation
Threat	Asset, adversary and verification setting	Catalogue description only until evidence is linked
Feature	Overt/covert/forensic mechanism and dose	Control process variables and change triggers
Verification	Instrument, decision rule and ageing	Report method, result, uncertainty and limits
System	UDI/traceability role and final-product evidence	Apply final acceptance and responsibility boundary

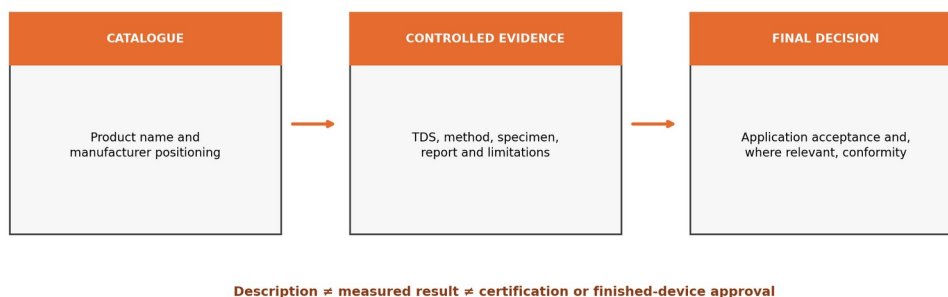


Figure 2. WP-21 separates catalogue positioning, measured evidence and final application decisions.

KEY INSIGHT

Precise product or application language is retained only when the exact formulation, method, processed specimen and controlled evidence can be traced.

5. Limitations

- No material feature is uncopyable or universally secure.
- UDI and authentication are not interchangeable.
- A marker does not establish MDR or market-surveillance compliance.
- Security performance depends on infrastructure and secrecy.
- Final-formulation evidence must be reassessed.

6. Conclusions

- Thermochromic, photochromic, fluorescent and infrared features are tools within a security architecture.
- Effectiveness requires threat modelling, controlled verification and resistance-to-copy testing.
- Adding a marker changes the formulation and can alter optical, mechanical, chemical and biological evidence.
- This corrected candidate remains local and on HOLD until series-wide scientific, metadata and visual release checks are complete.

Revision note

Version 5.3 removes unsupported legal requirements and economic figures, separates UDI/serialization/track-and-trace/authentication, and adds threat-model and final-formulation validation gates.

Acknowledgements. The author acknowledges the 3Dresyns technical team and users whose manufacturing experience informed this correction.

Disclosure. Dr. Juan Segurola is founder and Scientific Director of 3Dresyns by Resyner Technologies S.L., the supplier of the materials discussed.

References

- [1] 3Dresyns. Current security-feature product TDS and controlled verification reports.
- [2] Regulation (EU) 2017/745 on medical devices, current consolidated version and UDI provisions.
- [3] Regulation (EU) 2019/1020 on market surveillance and compliance of products.
- [4] ISO 12931:2012. Performance criteria for authentication solutions used to combat counterfeiting of material goods.
- [5] ISO/IEC 15459 series. Automatic identification and data capture techniques—Unique identification.
- [6] Ligon, S. C. et al. (2017). Polymers for 3D printing and customized additive manufacturing. <https://doi.org/10.1021/acs.chemrev.7b00074>