

Bilion dolarów, który znika. I jak druk może to zatrzymać

MultiDot Secure, Cyfrowy Paszport Produktu wyścig zbrojeń z fałszerzami

Kategoria: Zabezpieczenia i ochrona marki | Czas czytania: ok. 8 minut

Rynek podróbek jest wart od 467 miliardów do jednego biliona dolarów rocznie i rośnie w ogromnym tempie: 12–18% rok do roku. To więcej niż budżet niejednego państwa europejskiego. Jednocześnie technologie zabezpieczeń – od hologramów po kody QR – mają coraz większe problemy z nadążeniem za kreatywnością fałszerzy. Potrzebna była nowa klasa zabezpieczeń. I pojawiła się – zaszyta w strukturze rastra.

Skala problemu: liczby, które porażają

Podróbki nie są problemem tylko dla luksusowych marek. Dotykają praktycznie każdej branży:

Branża	Szacowane straty roczne	Ryzyko dla konsumenta
Farmaceutyki	200 mld USD	Bezpośrednie zagrożenie zdrowia i życia
żywność i napoje	49 mld USD	Zatrucia, nieznana zawartość
Elektronika	100 mld USD	Niebezpieczne baterie, pożary, niska trwałość
Dobra luksusowe	98 mld USD	Strata finansowa, fałszywa ekskluzywność
Motoryzacja	15 mld USD	Fałszywe poduszki powietrzne
Alkohol i tytoń	40–50 mld USD	Alkohol metylowy, nieznane składniki

Jak przypomina Tomasz Jasiński – problem jest głęboko ludzki:

„Jeżeli kupimy produkt, który jest nieprawdziwy – na przykład alkohol metylowy w opakowaniu zwykłego alkoholu – to może się to odbić na zdrowiu i może skończyć się tragicznie.”

Dlaczego dotychczasowe metody nie wystarczają?

Dwie szkoły zabezpieczeń

Andrzej Kunstetter wyróżnia dwa podstawowe podejścia do ochrony przed fałszerstwem:

Szkoła jawna: producent otwarcie mówi „tu jest zabezpieczenie, spróbuj je podrobić” – hologram, znak wodny, specjalna folia. Skuteczność zależy od jakości technicznej.

Szkoła ukryta: zabezpieczenie jest niewidoczne, a wiedza o tym, gdzie i jak jest zastosowane, stanowi klucz. Na przykład celowo „uszkodzona” litera, która wygląda jak błąd drukarski – jeśli fałszerz nie wie, że to element zabezpieczenia, skopiuje ją jak resztę lub „naprawi”.

Najskuteczniejsze systemy – jak banknoty – łączą oba podejścia: część zabezpieczeń jest widoczna i znana, część pozostaje tajna. MultiDot Secure należy do tej drugiej kategorii – z tą różnicą, że działa w strukturze samego druku.

Problem z tradycyjnymi kodem QR i DPP

Od 2025 roku Unia Europejska stopniowo wprowadza obowiązek stosowania Cyfrowego Paszportu Produktu (DPP). Każdy produkt musi posiadać kod 2D – QR lub DataMatrix – z danymi o składzie, śladzie węglowym i łańcuchu dostaw danego produktu.

Cyfrowy Paszport Produktu (DPP) – co to jest?

DPP to cyfrowy zestaw danych towarzyszący produktowi od produkcji po recykling. Zawiera informacje o składzie, śladzie węglowym, możliwościach naprawy i ponownego użycia. Dostępny poprzez zeskanowanie kodu QR lub DataMatrix. Wymagany unijnym rozporządzeniem ESPR. Pierwsze obowiązkowe wdrożenia: baterie od 2027 r., następnie tekstylia i elektronika.

Problem jest jednak oczywisty, jak przyznają eksperci Heidelberg Polska:

*„Kod QR czy DataMatrix to zwykły kod 2D. Można go absolutnie zeskanować, skopiować i wstawić na zupełnie inny produkt. –
Tomasz Jasiński”*

Oznacza to, że DPP świetnie sprawdza się do śledzenia łańcucha dostaw, ale **sam w sobie nie chroni przed podrabianiem**. Etykieta z kodem może być zeskanowana lub wygenerowana od nowa i wydrukowana na innym produkcie. Potrzebna jest dodatkowa warstwa ochronna.

MultiDot Secure: zabezpieczenie ukryte w strukturze druku

MultiDot Secure to technologia budowana na fundamencie podstawowej wersji MultiDot. Zamiast jednak stosować dodatkowe folie, hologramy czy inne skomplikowane procesy, zabezpieczenie jest **zakodowane**

bezpośrednio w strukturze rastrowej obrazu – w sposób niewidoczny gołym okiem.

Jak to działa:

- **Ukrycie:** specjalny moduł programowy koduje wybrany unikalny obraz (np. logo, kod, wzorec o miliardach kombinacji) bezpośrednio w strukturze rastrowej.
- **Weryfikacja:** osoba sprawdzająca – inspektor, celnik, właściciel marki – wie, w którym miejscu szukać, i patrzy przez specjalne szkło powiększające.
- **Potwierdzenie:** system porównuje to, co widzi, ze wzorcem. Kod ma 17 miliardów kombinacji – skopiowanie go bez wiedzy o „kluczu” jest praktycznie niemożliwe.

Kluczowa zaleta: **nie wymaga żadnych dodatkowych materiałów ani osobnych procesów w drukarni**. Zabezpieczenie powstaje podczas standardowego procesu drukowania. Wzrost kosztu odbitki: zerowy.

Jak MultiDot Secure uzupełnia DPP?

Wyobraźmy sobie opakowanie z kodem QR – wymaganym przez unijne rozporządzenie. Falszerz kopiuje etykietę i przenosi ją na swój produkt. System śledzenia notuje, że kod jest „prawdziwy”, bo pochodzi od oryginalnego producenta. Konsument nie wie, że kupuje podróbkę.

Z MultiDot Secure:

- Kod QR/DataMatrix pełni nadal swoją wymaganą przepisami rolę logistyczno-informacyjną.
- Ukryta warstwa w strukturze rastra jest niepowtarzalna dla każdej serii opakowań.
- Skopiowanie etykiety czy ponowne wygenerowanie kodu nie kopiuje ukrytego wzorca – jest on powiązany z konkretną formą drukową, nie z obrazem.

„DPP daje dane, a MultiDot Secure daje dowód, że to nie jest „zdjęcie danych”.”

Porównanie metod zabezpieczeń

Metoda	Koszt wdrożenia	Skuteczność	Dodatkowy proces?
Hologramy tęczowe	Wysoki	Średnia (falszerze mają sprzęt)	Tak
RFID / NFC	Bardzo wysoki	Bardzo wysoka	Tak

Metoda	Koszt wdrożenia	Skuteczność	Dodatkowy proces?
Kody QR z unikalnym ID	Niski	Średnia (możliwa kopia)	Nie
Etykiety VOID / destrukcyjne	Średni	Średnia (jednorazowe)	Tak
Mikrodruk / gilosz	Wysoki	Niska (kopiowane)	Tak
MultiDot Secure	Średni	Bardzo wysoka	Nie

Na jakim etapie jest technologia?

MultiDot Secure jest dziś w fazie prototypowej – działającej, ale jeszcze nie we wdrożeniu masowym. Zespół pracuje nad finalizacją specjalizowanego skanera weryfikacyjnego oraz uproszczeniem procesu wdrożenia dla właścicieli marek. To technologia, która wchodzi dokładnie w tym momencie, w którym DPP staje się obowiązkowy.

Tomasz Jasiński nie kryje optymizmu:

„Jesteśmy w stanie do cyfrowego paszportu dodatkowo dodać warstwę zabezpieczającą, która uniemożliwi cyfrowy paszport produktu podrobić.”

Podsumowanie

- **Rynek podróbek** rośnie do 12–18% rocznie i jest wart nawet bilion dolarów.
- **Cyfrowy Paszport Produktu (DPP)** jest obowiązkowy od 2025–27 roku, ale sam w sobie nie chroni przed podrabianiem.
- **MultiDot Secure** koduje unikalną warstwę informacyjną bezpośrednio w strukturze rastrowej – bez dodatkowych materiałów i bez wzrostu kosztu druku.
- **Dwie szkoły zabezpieczeń:** jawna (hologram, kod) i ukryta (zaburzona struktura). MultiDot Secure należy do tej drugiej – najskuteczniejszej, a w zasadzie łączy obie.
- **Skuteczna ochrona marki** = DPP (identyfikacja) + MultiDot Secure (dowód autentyczności).
- **Technologia jest w fazie prototypowej**, z docelowym wdrożeniem komercyjnym.

Szczegóły dotyczące wdrożenia MultiDot Secure są dostępne bezpośrednio u Andrzeja Kunstettera i Tomasza Jasińskiego z Heidelberg Polska.