

Da identificação à prova

Como escolher a tecnologia de autenticação adequada para cada produto físico

Rafael Kohler Costa | Founder, Tagstrust Tecnologia

Quando uma empresa decide conectar um produto físico ao ambiente digital, a primeira pergunta costuma ser qual tecnologia usar. QR Code, código de barras, RFID, NFC, impressão de segurança ou uma combinação entre essas alternativas? A resposta não depende apenas de custo, alcance ou facilidade de leitura. Depende, sobretudo, do que precisa ser comprovado.

Há produtos para os quais basta oferecer acesso rápido a informações. Em outros casos, é necessário individualizar cada unidade, acompanhar sua circulação, identificar indícios de duplicação, registrar uma abertura ou verificar, de forma dinâmica, se o elemento apresentado é autêntico. Quanto maiores o risco, o valor e a relevância do produto, maior tende a ser a necessidade de evidências capazes de sustentar a confiança.

Antes da tecnologia vem a pergunta

Comparações tecnológicas perdem qualidade quando tratam todas as soluções como se respondessem ao mesmo problema. Identificação, serialização, autenticação, integridade e rastreabilidade são capacidades relacionadas, mas não equivalentes.

Identificar significa dizer quem ou o que determinado objeto afirma ser. Serializar significa atribuir uma referência própria a cada unidade. Autenticar exige verificar se aquela identidade é legítima. Integridade acrescenta evidências sobre abertura, violação, substituição ou transferência. Rastreabilidade organiza eventos que ajudam a compreender por onde o produto passou, quando foi lido e o que ocorreu ao longo de sua trajetória.

Há ainda uma distinção decisiva entre autenticar um identificador e autenticar o produto. Uma plataforma pode confirmar que determinado código, padrão gráfico ou chip é legítimo. Para que essa confirmação sustente uma conclusão sobre o objeto físico, é preciso demonstrar como o identificador foi associado à unidade e como esse vínculo é preservado ou revela sinais de alteração.

Uma solução pode cumprir muito bem uma dessas funções e não realizar as demais. Isso não significa que uma tecnologia seja sempre superior à outra. Significa que elas podem ter sido escolhidas para objetivos, escalas, custos e experiências de uso diferentes. A decisão deve considerar essas variáveis, mas também os limites tecnológicos relevantes em cada

caso. Por isso, a escolha não deve começar pela tecnologia mais conhecida ou pela promessa de maior segurança. Deve começar pela definição da prova necessária.

Códigos visuais e acesso simples à informação

Códigos de barras e QR Codes são recursos eficientes, acessíveis e amplamente reconhecidos. Podem conectar uma embalagem a uma página, a dados de lote, instruções, campanhas, informações regulatórias ou experiências digitais. Como são lidos pela câmera do celular, oferecem uma jornada simples e de baixo atrito para o consumidor.

Quando o mesmo código é aplicado a todas as unidades de um produto, ele normalmente identifica uma referência comercial, uma campanha ou uma página, mas não diferencia cada item físico. Nesse cenário, reproduzir a imagem do código também reproduz o caminho digital

que ele contém. O sistema pode continuar funcionando perfeitamente, mesmo que o código tenha sido copiado e aplicado em outro objeto.

A serialização eleva essa capacidade. Um código individual pode associar cada unidade a um registro próprio, permitir controle de ativações, comparar leituras e detectar comportamentos improváveis. A expressão QR dinâmico, porém, exige cuidado: em muitas implementações, o símbolo impresso permanece estático e o que muda são o destino, as regras ou a resposta da plataforma. A imagem continua visível e pode ser fotografada ou reproduzida. O sistema pode identificar reutilizações e gerar inteligência, mas isso não comprova, por si só, que o objeto no qual o código aparece seja autêntico.

Impressões de segurança e características físicas

Tecnologias ópticas podem explorar microtextos, elementos holográficos, padrões aleatórios, variações do processo de impressão ou características físicas difíceis de reproduzir. Quando cada marcador apresenta uma assinatura própria, uma câmera e um sistema de análise podem comparar a imagem capturada com uma referência previamente cadastrada.

Essa abordagem pode elevar significativamente a dificuldade de cópia e manter a leitura acessível por smartphone. Seu desempenho, porém, depende do elemento utilizado, da qualidade de impressão, do processo de cadastro, das condições de captura, do modelo de análise e da forma como o marcador permanece ligado ao produto. A autenticação do marcador também precisa ser distinguida da comprovação automática do conteúdo da embalagem.

RFID UHF e eficiência operacional em escala

Etiquetas RFID passivas UHF são especialmente valiosas quando a operação exige leitura sem contato visual direto, identificação de vários itens em sequência e automação de

inventários, recebimentos, expedições e movimentações logísticas. Em ambientes industriais, essa capacidade pode reduzir intervenções manuais e ampliar a visibilidade sobre o fluxo dos produtos.

RFID, entretanto, designa uma família de tecnologias, da qual o próprio NFC faz parte em outra faixa e com outra experiência de uso. Uma etiqueta UHF que apenas transmite um identificador não oferece necessariamente autenticação criptográfica. A resistência à clonagem, o alcance, a privacidade e a proteção dos dados dependem do chip, do protocolo, da configuração e da arquitetura. Operações UHF em escala também costumam exigir leitores e antenas próprios, investimento coerente com processos de alto volume, mas diferente da jornada de verificação pelo celular.

NFC pode ser apenas um link ou produzir uma prova

O NFC aproxima o produto da experiência cotidiana do consumidor. Em muitos celulares, basta encostar o aparelho na etiqueta para abrir uma página ou iniciar uma verificação. A etiqueta pode operar sem bateria, recebendo energia do próprio campo de leitura.

Mas a presença de NFC, sozinha, não define o nível de segurança. Uma etiqueta simples pode armazenar apenas um endereço eletrônico e cumprir função semelhante à de um QR Code. Já um componente criptográfico pode proteger chaves e gerar respostas variáveis a cada interação. Nesse modelo, a plataforma envia ou interpreta um desafio, valida a resposta produzida pelo chip e verifica se ela poderia ter sido gerada por uma credencial legítima.

Essa diferença é fundamental. Em uma implementação criptográfica corretamente projetada, copiar o endereço, o identificador visível ou a aparência da etiqueta não reproduz a chave protegida nem a resposta esperada. A verificação deixa de depender apenas de uma informação estática e passa a exigir uma prova dinâmica. Ainda assim, a força do conjunto

depende do componente, da gestão das chaves, do protocolo, da validação no servidor e do vínculo físico com o produto.

Autenticar a identidade não basta se o vínculo físico se perder

Mesmo uma identidade digital forte precisa permanecer associada ao produto correto. Se uma etiqueta autêntica puder ser removida de uma embalagem e transferida para outra sem deixar evidência, o sistema poderá reconhecer corretamente a etiqueta, mas não necessariamente o objeto ao qual ela foi posteriormente vinculada.

É nesse ponto que entram os mecanismos de integridade. Materiais destrutíveis, microcortes, adesivos adequados, estruturas de lacre e recursos capazes de registrar uma abertura ajudam a preservar a relação entre identidade e produto. O objetivo não é

declarar que um objeto físico se tornou inviolável, e sim produzir evidências verificáveis quando essa relação é alterada.

Essas evidências também não equivalem, isoladamente, a uma análise da composição ou da qualidade do conteúdo. Elas fortalecem a confiança sobre identidade, vínculo e estado observável da embalagem. A segurança do produto continua dependendo dos controles de fabricação, distribuição, armazenamento, inspeção e qualidade aplicáveis ao caso.

A tecnologia ganha valor quando integra uma infraestrutura

O identificador é apenas a porta de entrada. Para transformar uma leitura em confiança operacional, é necessário interpretar contexto: quando ocorreu, em qual local, qual era o estado esperado do produto, quais eventos vieram antes e que comportamento aquela interação representa. Trata-se de rastreabilidade baseada em eventos registrados nas interações, e não de acompanhamento contínuo ou localização em tempo real quando não há leitura.

Uma infraestrutura bem construída pode reunir identidade individual, autenticação, estado de integridade, histórico de eventos, regras de negócio, integrações com sistemas corporativos e análise de anomalias. Também pode separar informações públicas, destinadas ao consumidor, de dados operacionais e evidências reservadas à marca.

Nesse ambiente, inteligência artificial e análise de dados não substituem a autenticidade do identificador. Elas ampliam a capacidade de interpretar eventos confiáveis, reconhecer padrões e priorizar situações que merecem investigação. A qualidade da inteligência depende da qualidade das identidades e dos registros que a alimentam.

VERA™ Tagstrust: a arquitetura desenvolvida pela Tagstrust

Uma das soluções desenvolvidas pela Tagstrust nasce dessa visão integrada. Essa arquitetura recebe o nome de VERA™ Tagstrust — Vínculo, Evidência, Rastreabilidade e Autenticidade.

O nome traduz os quatro elementos que orientam sua concepção: preservar o vínculo entre a identidade digital e o produto físico; produzir evidências verificáveis sobre identidade e integridade; registrar eventos que sustentem a rastreabilidade ao longo da trajetória; e permitir a verificação da autenticidade por mecanismos compatíveis com o nível de risco da aplicação.

Sua inovação não está em reivindicar a exclusividade de cada componente isolado, mas na arquitetura própria que os organiza para situações em que a marca precisa ir além do acesso à informação e preservar, ao longo do tempo, a continuidade do vínculo entre uma identidade digital legítima e o produto físico correto.

A VERA™ Tagstrust combina identidade única por unidade, autenticação criptográfica baseada em componente seguro, leitura por aproximação com celulares compatíveis, mecanismos físicos de integridade, registro de eventos e conexão com uma infraestrutura de dados preparada para rastreabilidade e inteligência. Cada camada responde a uma pergunta diferente: a identidade

distingue a unidade; a criptografia permite verificar a legitimidade do elemento; os mecanismos físicos ajudam a evidenciar alterações; e os eventos preservam contexto sobre a trajetória.

A camada de dados e inteligência correlaciona essas evidências, aplica regras de negócio e ajuda a reconhecer padrões de uso, duplicidade ou anomalia. Ela não transforma um identificador fraco em prova forte; seu valor aumenta quando recebe eventos provenientes de identidades e mecanismos de validação confiáveis.

Essa proposta não pretende substituir tecnologias escolhidas para finalidades distintas. Um código visual pode ser plenamente adequado para informar, engajar ou oferecer acesso simples. RFID UHF pode ser a escolha mais eficiente para inventário e automação logística. A VERA™ Tagstrust se torna especialmente adequada quando o risco ou o nível de controle pretendido exige autenticação forte, evidências de integridade e continuidade verificável entre o registro digital e o objeto físico.

A arquitetura também preserva espaço para interoperabilidade. A identidade do produto pode dialogar com padrões de rastreabilidade, sistemas corporativos e experiências digitais, sem confundir o acesso à informação com a prova de autenticidade.

Para que empresas avaliem essa proposta fora de uma apresentação teórica, a campanha piloto Tagstrust 90 dias foi concebida como uma experiência em ambiente real. O objetivo é permitir que cada organização observe a jornada de verificação, os dados gerados e a aderência da arquitetura ao seu próprio risco, processo e produto. O piloto não substitui critérios de homologação ou ensaios específicos; ele cria condições concretas para uma decisão mais bem informada.

Segurança proporcional ao que precisa ser comprovado

A infraestrutura de confiança não precisa ser igual para todos os produtos. Ela pode ser pensada de forma proporcional ao risco, ao valor e à relevância daquilo que precisa ser comprovado.

Para uma campanha informativa, um QR Code pode ser a escolha mais eficiente. Para controle logístico em grande escala, RFID UHF pode trazer ganhos difíceis de alcançar por leitura individual. Para produtos sujeitos a falsificação, substituição, reenvase, desvio ou exigências regulatórias, a combinação entre identidade individual, autenticação dinâmica, evidências de integridade física e registro de eventos pode oferecer uma base de verificação mais robusta.

Nenhuma tecnologia elimina isoladamente todos os riscos. A proteção nasce da coerência entre o problema, o elemento físico, o mecanismo de validação, os dados registrados e a forma como o resultado é comunicado. O nível de confiança não deve ser presumido pelo nome da tecnologia. Precisa ser demonstrado pelo que ela efetivamente consegue verificar.

Informar adequadamente clientes e consumidores sobre o alcance e as limitações da solução é parte da própria infraestrutura de confiança. A comunicação deve permitir compreender o que foi verificado, em quais condições e o que permanece fora do escopo. Confiança verificável também começa pela precisão daquilo que se divulga.

Da conexão à confiança verificável

A evolução da identidade de produtos não está apenas em adicionar um código ou uma etiqueta à embalagem. Está em compreender que cada interação pode representar um nível diferente de evidência.

Conectar permite acessar. Individualizar permite distinguir. Autenticar permite comprovar a legitimidade da identidade. Verificar integridade permite reconhecer alterações relevantes. Registrar eventos permite compreender a trajetória. Quando essas capacidades são combinadas de acordo com o risco, a confiança deixa de depender apenas de uma declaração e passa a ser sustentada por evidências.

É nesse espaço que a Tagstrust atua: construindo uma infraestrutura capaz de preservar e testar a relação entre a identidade digital e o produto físico, para que marcas, cadeias produtivas e consumidores disponham de evidências compatíveis com aquilo que precisam verificar.

Síntese das capacidades

A tabela resume capacidades típicas. O desempenho real depende da implementação, dos componentes e da arquitetura adotada.

Tecnologia	Contribuição principal	Limitação típica
Código de barras ou QR estático	Acesso simples a informações e identificação de referência	O símbolo visível pode ser reproduzido e normalmente não individualiza cada unidade
QR serializado com lógica dinâmica	Identidade individual, regras de acesso, análises e detecção de reutilização	O símbolo impresso pode ser copiado; a força depende da plataforma e da análise de contexto
Impressão de segurança	Eleva a dificuldade de reprodução e pode criar assinatura física própria	Depende do marcador, da captura, do cadastro e do vínculo com o produto
RFID passivo UHF	Automação logística e leitura em escala sem contato visual direto	Segurança varia conforme o chip e normalmente requer infraestrutura específica
NFC simples	Interação por aproximação e acesso fácil a uma experiência digital	Pode funcionar apenas como portador de uma informação estática
NFC com recursos criptográficos	Prova dinâmica com chave protegida e validação pelo sistema	Depende do protocolo, da gestão de chaves, do vínculo físico e da infraestrutura

Como avaliar uma solução

Uma comparação responsável começa pelo risco e pela evidência necessária. Antes de escolher a tecnologia, convém definir se a organização precisa apenas disponibilizar informação, distinguir unidades, verificar uma credencial, reconhecer sinais de abertura, acompanhar eventos ou combinar essas capacidades.

Em seguida, é importante observar o que de fato é validado. O resultado se refere ao código, ao chip, à etiqueta, à embalagem ou ao produto? Como o identificador é vinculado à unidade? O que acontece se ele for copiado, removido ou transferido? Quais eventos são registrados e quem consegue consultá-los?

Por fim, o desempenho deve ser analisado no ambiente real. Materiais, formato da embalagem, processo de aplicação, aparelhos de leitura, conectividade, gestão de chaves, integrações e comportamento dos usuários podem alterar o resultado. Uma porcentagem isolada ou o nome de uma tecnologia não substituem a definição da métrica, do método de ensaio, do escopo e das condições de uso.

Esse roteiro permite reconhecer o mérito de soluções diferentes e, ao mesmo tempo, identificar quando o risco exige uma arquitetura mais completa. A escolha deixa de ser uma disputa entre etiquetas e passa a ser uma decisão sobre quais evidências a organização precisa produzir e preservar.

Referências para aprofundamento

NFC Forum Technical Overview
 RAIN Alliance What is RAIN RFID
 GS1 GS1 Digital Link
 GS1 EPCIS and CBV
 ISO ISO 22383 2020
 NXP NTAG 424 DNA