

Evaluating Smartphone authentication

A buyer's guide for security printers, brand owners and revenue authorities

Quantum Base

Evaluating smartphone authentication

A buyer's guide for security printers, brand owners and revenue authorities.

In this guide

Why this guide exists 2

Which smartphone devices does it work on, and how do you know? 3

What happens outside the lab? 4

What does an authentication system do when it cannot be sure? 5

What security evidence can you show? 6

Will people actually use it? 7

Where does it not work? 8

The evaluation checklist 9

About Quantum Base 10

Why this guide exists

Smartphone authentication is moving from concept to global deployment. Two industry shifts are driving it. GS1 will phase out traditional 1D barcodes in favour of 2D barcodes by the end of 2027, and digital product passport legislation is putting more product information behind QR codes. More phone readable codes on more products, scanned by more people.

That creates a problem. A QR code links to information; but it doesn't verify the product it's printed on. Photocopy a QR code, even an encrypted one, and the duplicate scans exactly like the original. A counterfeit carrying a copied code doesn't just get past the check, it passes it the same as the original. As QR codes spread across packaging, buyers are realising they need something that proves the item is genuine, not just that the code exists.

The market has recognised what this means: with billions of smartphones already in people's hands, authentication can finally operate at the same scale as the counterfeit problem. But not all systems are created equal. The truth is that smartphone authentication solutions need to work on a wide range of devices, in a wide range of lighting conditions, for a wide range of users, on a wide range of products - whilst still being secure and easy to use.

This guide sets out six questions to put to any supplier of smartphone authentication. None are trick questions and none are proprietary. They are the questions our own scientists would ask if they were buying rather than building.

If a supplier can answer all six with evidence, you are looking at a serious solution. If they cannot, you have learned something useful before spending a dime.

Which smartphone devices does it work on, and how do you know?



Phones vary enormously. Different sensors, cameras, lenses, flashes, image processing, software and operating systems. Two models in the same family from the same manufacturer can capture the same feature differently.

That single fact undoes most of what gets claimed in the smartphone authentication category. A supplier who says “it works on smartphones” has told you nothing about whether it will work on the handsets your inspectors, distributors and customers actually carry. Those devices vary widely by region, price point and age, with different cameras, operating systems and manufacturer software. Performance on a current flagship says little about performance on an older budget model, and in many markets, that’s the phone most people have.

Ask for:

01 A maintained list of supported devices, not a claim of universal coverage.

02 How those devices were tested, and how often testing is repeated.

03 What happens when a handset receives an operating system update, or a manufacturer changes its camera software.

04 An honest statement of which devices cannot be supported reliably.

That last one matters most. A supplier willing to name what doesn’t work is describing a real product. A supplier claiming everything works has either not tested widely or may have lowered the acceptance threshold for security. You want to understand if wide device compatibility increases the chance of a counterfeit being accepted as genuine.

What happens outside the lab?

In a laboratory the samples are clean, the lighting is controlled and the operator knows exactly what to do. None of that describes a warehouse, a shop floor, a border post or a customer's kitchen.

In the field, a product might be scanned in bright sunlight, in a dark warehouse, or under fluorescent light. Packaging might be curved, reflective, dirty or damaged. The phone might be moving, or held at the wrong angle. Optical methods of authentication are particularly sensitive to lighting and camera behaviour, but every security feature has its own version of this problem.

A solution that performs beautifully on a flat, pristine label can behave very differently on curved, handled packaging that has been through heat, moisture and a real-world supply chain.

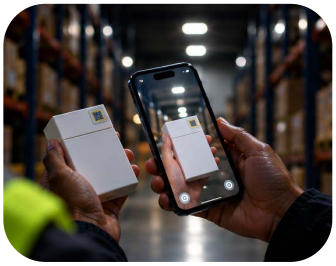
Environmental scanning conditions



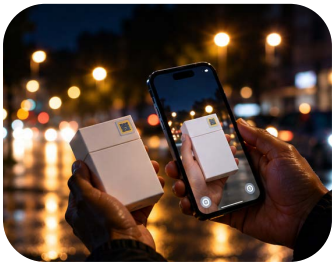
Bright daylight



Bright artificial light



Dark warehouse



Outdoor night

Packaging scanning variations



Curved



Dirty



Reflective



Damaged

Ask for:

01 Test results from the conditions your programme will actually involve, not from a controlled demonstration.

02 Evidence that the system judges its own capture quality and asks for another attempt when the evidence is weak.

03 How the system guides a user who is getting it wrong.

04 Results on your substrates, your finishes and your product shapes.

The underlying principle is that the phone, the ambient environment, the illumination, the material response and the decision software form a single chain. They cannot be engineered or tested independently. A supplier who talks only about their security feature, and not about the chain it sits in, has tested half the problem.

What does an authentication system do when it cannot be sure?

Most buyers assume authentication has two outcomes. Genuine, or counterfeit. A well-built system has three.



- Authenticated as genuine.
- Flagged as a potential counterfeit
- Not enough evidence to decide.

The third outcome is the one that tells you whether a supplier is serious. A poor scan must not quietly become a counterfeit verdict, and it certainly must not become a genuine one.

A system that always produces a verdict is not more desirable than one that sometimes declines - it is less trustworthy. Its important that a system can understand both signal and noise, especially in real world conditions.

Ask for:

01	Confirmation that an inconclusive result is a designed outcome, not an error state.
02	What the user is shown and asked to do when it happens.
03	How often it happens, across devices and conditions.
04	What the escalation route is for an item the system cannot resolve.

The safe system is not the one that always gives an answer. It is the one that knows when the evidence is not strong enough, and says so.

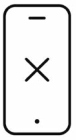
What security evidence can you show?

Start with threat models. The term sounds heavier than it is. A threat model simply identifies who the counterfeiter is, what they are trying to gain, and what equipment and knowledge they have. It sets the bounds of an attack.

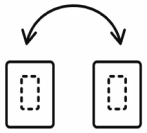
For each threat model, a supplier should have tested the attacks that matter to it:



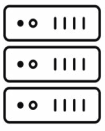
Reproducing the feature on counterfeit packaging, including photocopies and high fidelity re-creations.



Emulating the feature's response, such as screen replay, synthesised images, or injecting recorded scans directly into the app.



Transferring a genuine label from a real product onto a counterfeit one.



Attacking the app and the back-end database rather than the physical feature

That last category is routinely overlooked. Strong physical features can be undermined by weak registration, a compromised app or poor back-end controls. If an attacker has the back end, the physics no longer matters.

Borrow the measurement discipline from biometrics

Product authentication doesn't need to start from scratch. Fingerprint and face recognition have spent decades developing standards and testing methods for a similar challenge; distinguishing genuine users from impostors, both reliably and consistently. We should learn from that experience and adapt those approaches to authenticating products.

The central lesson is simple: one accuracy figure is not enough. Suppliers should report separately how often counterfeits are accepted, genuine products are rejected, and the phone cannot obtain a usable scan. Testing should also show how these results change across phones and conditions, and whether stricter checks keep out more counterfeits at the cost of rejecting more genuine products.

Established approaches to shared specifications, independent testing and certification offer a useful model too. We should build on this work, so buyers can compare evidence and not navigate a different definition of reliability from every supplier.

Existing standards include **ISO 19795** for measuring biometric performance; NIST's face-recognition evaluations for comparing error rates; and **FIDO2** for shared specifications and certification.

Ask for:

01 The threat models considered, and the attacks tested against each.

02 Error rates reported separately, at stated thresholds, under stated conditions.

03 Who has independently verified those figures.

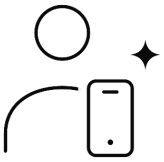
04 How the back end, the reference data and the app itself are protected, and who has access.

Will people actually use it?

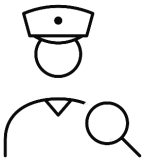
Usability is not a nice-to-have sitting alongside security. It is a security property. If a process is slow, confusing or unreliable, people stop using it or work around it, and a system nobody uses offers no protection at all.

The goal is to make the secure action the obvious action and the easiest action. In practice that means a simple experience, clear instructions, a fast response, and helpful guidance when something goes wrong. The system should detect as much as it can automatically, rather than requiring the user to understand anything about the technology underneath.

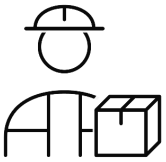
Different users need different things:



A consumer might scan once, in a shop, having never seen the feature before.



An inspector might scan hundreds of items in a session and needs speed above all.



A warehouse operator might be wearing gloves, working quickly, with poor connectivity inside a large building.

The experience has to be tested with those people, in those conditions. Testing it with engineers in an office produces results that do not transfer to real world implementations.

Ask for:

01 Evidence of testing with untrained users in realistic conditions.

02 Measurement of the whole journey: how many people start a scan, how many need to retry, how long it takes, where people give up.

03 Which languages the app, on-screen guidance and error messages support, and whether the experience has been tested with native speakers in your target markets, not just translated.

04 What the supplier does when those numbers look bad.

That final question is the one that separates good suppliers from the rest. When a journey is failing there are two ways to fix it: improve the system; or lower the security. The first is engineering. The second is a security failure reported as a usability improvement.

Where does it not work?

No anti-counterfeiting system works everywhere, on everything, against every threat. A credible supplier is clear about the boundaries of what they sell. An evasive answer here is the most informative answer in the whole evaluation.

There are real limits worth understanding. An NFC tag will not work through a ferrous barrier. An optical method will not work if the object is obscured, the image is too blurred, or there is too much background light. Even a QR code is an optically read technology and fails when the camera cannot capture it cleanly.

There are also limits that come from outside the security supplier entirely. A manufacturer pushes a software update to a two-year-old handset, a camera interface changes, capture quality drops, and compatibility work has to be redone. The breadth of smartphone manufacturers and devices is a genuine constraint on this whole category.

Before you deploy

- Start with your real use cases, not the supplier's demonstration.
- Which phones and operating systems must you support?
- Will people be scanning indoors, outdoors or with poor data connectivity?
- What materials, shapes and finishes are involved?
- Could a genuine label be moved from a real product onto a counterfeit one?
- What happens if a user's phone is compromised or unpatched?
- How is reference data protected, and who has access to it?

Then run a print trial with real products, real users and real conditions. Agree in advance what success means: acceptable rates for wrong acceptances, wrong rejections and unreadable scans; an acceptable response time; the device coverage you need; the support you expect. Agree the escalation route for items the system cannot resolve.

And hold on to the wider point. Authentication sits alongside traceability, tamper evidence, enforcement and user education. It does not replace them.

The right question is not "does this work?" It is: where does it work, against what attacks, with what evidence, and what happens when it cannot work?

Broad Smartphone compatibility

"A demonstration on a single device proves an idea is possible.
Consistent results across a tested range prove a solution is deployable."

Professor Rob Young, Chief Scientific Officer, Quantum Base

The evaluation checklist

Supplier _____ Date _____

Device coverage

- Maintained list of supported devices provided
- Test method and testing frequency explained
- Process for OS and manufacturer software updates described
- Unsupported devices explicitly named.

Real-world conditions

- Results shown from field conditions, not controlled demonstration
- System judges its own capture quality
- User guidance demonstrated, not described
- Tested on own substrates, finishes and product shapes

Inconclusive results

- “Not enough evidence” exists as a designed outcome
- Frequency of that outcome disclosed, by device and condition
- Escalation route defined for unresolved items

Security evidence

- Threat models stated
- Attacks tested per threat model, including label transfer and back-end attack
- Error rates reported separately, at stated thresholds and conditions
- Independent verification named
- Back-end, reference data and app security explained; access controls stated

Usability

- Tested with untrained users in realistic conditions
- Whole-journey metrics available: starts, retries, duration, abandonment
- Supplier’s response to poor journey metrics is engineering, not threshold reduction

Limits and deployment

- Supplier states clearly where the solution does not work
- Print trial agreed with real products, users and conditions
- Success criteria agreed in writing before the trial begins
- Integration with traceability, tamper evidence and enforcement understood

Scoring it: any supplier can produce a confident answer. You are listening for evidence, and for a willingness to name limits. A supplier who cannot tell you where their product fails has not tested it hard enough to know.

About Quantum Base

We wrote this guide because we are asked these questions, and because we think more buyers should be asking them.

Quantum Base makes Q-ID®, a physics-based authentication optical feature that prints like an ordinary ink at production speed and is read with a smartphone. We spun out of Lancaster University and are listed on the London Stock Exchange. Two billion Q-IDs are already protecting products would wide, and we hold 40+ patents granted or pending.

We publish our science in peer-reviewed papers, and our scientists will talk to yours directly.

If you want to put the six questions to us, we will answer them on the record. If you would rather test it than discuss it, we will send you printed samples to scan on your own phone, on your own network.

Request a sample →

Talk to the team →

Read the research →

Impossibly Simple. Atomically Secure.