Disguised Security Technology™ (DST) Standard

Version 1.1 — Professional Specification Edition

Prepared by: KeySpot Security Ltd
Author: Mark Cowie, Founder and Category Originator
Status: Foundational Category Standard
Classification: Security Engineering / Physical Security / Access Control

0. Overview

Disguised Security Technology™ (DST) defines the engineering, performance, and certification requirements for physical security devices whose primary protective function is concealment through environmental disguise.
DST establishes the world's first formalised structure for security products designed not to be visually recognised during typical observation, thereby reducing targeted criminal activity.

This standard sets out the minimum criteria for design, performance, testing, and compliance

necessary for a product to be recognised as a DST Certified™ Product.

1. Scope

This standard applies to all physical access security devices whose primary mechanism of protection relies on engineered visual disguise, including but not limited to:

- **Disguised key safes**
- **Disguised access panels**
- **Disguised smart lock housings**
- **Disguised service enclosures**
- **Disguised emergency access devices**
- **Hybrid concealed security products**

The standard does not apply to cosmetic disguises, decorative covers, or traditional security devices with visible locks or mechanisms.

2. Objective of the Standard

The DST Standard has been created to:

1. Establish a recognised benchmark for disguised physical security devices.
2. Differentiate DST products from visible, conventional security hardware.
3. Provide insurers, installers, and certification bodies with a reliable framework.

4. Ensure that disguise as a security principle is engineered, measurable, and testable.
5. Create a structured certification pathway (**DST Certified™) for compliance and auditing.**

3. Definition of Disguised Security Technology™

A product qualifies as DST when:

1. Concealment is an engineered, intentional design feature.
2. The product cannot be readily identified as a security device during typical observation.
3. Physical security properties remain equal to, or exceed, comparable visible devices.
4. Locking mechanisms, fixings, and structural components are not externally visible.
5. The product reduces or eliminates targeting risk through successful visual deception.
6. The product complies with applicable safety, access, and insurance requirements.

Disguise must be intrinsic to the product's engineering, not an aesthetic afterthought.

4. Core Principles of DST

4.1 Disguise Principle

The product must be purposefully engineered to resemble a non-security fixture common within its installation environment. This includes architectural elements, utility panels, or neutral surface features.

4.2 Security Engineering Principle

The disguise must not compromise structural integrity or security performance. Reinforcement, anti-pry geometry, internal shielding, and protected locking mechanisms are mandatory.

4.3 Compliance Principle

DST devices must consider and support relevant regulatory frameworks, including:

- **UK insurance expectations**
- **Police Preferred Specification criteria**
- **SBD alignment**
- **Fire and safety regulations**
- **International security standards where applicable**

4.4 Safety Principle

DST products must ensure:

- **Resistance to weather, corrosion, and UV**
- **Structural stability during long-term exposure**
- **No entrapment hazards**
- **Safe operation for authorised users**

---

5. Technical Requirements

5.1 Concealment Requirements

DST products must:

- **Present no external features identifying them as security devices.**
- **Contain no visible hinges, locks, mechanisms, or fixing points.**
- **Visually integrate with surrounding surfaces at typical viewing distances.**
- **Use colours, textures, and materials appropriate for realistic disguise.**

5.2 Structural Requirements

DST products shall:

- **Use materials appropriate for exterior installation or designated environments.**
- **Resist forced-entry attempts proportionate to their purpose.**
- **Provide internal shielding for locking mechanisms.**
- **Maintain structural integrity in all rated weather conditions.**

5.3 Operational Requirements

DST devices must:

- **Allow secure, reliable access for authorised users.**
- **Retain operational stability over long-term exposure.**

- **Include installation instructions preventing misapplication.**

5.4 Anti-Tamper Requirements

Minimum anti-tamper performance shall include:

- **Reinforced mounting architecture.**
- **Internal barriers to prevent probing, drilling, or prying.**
- **Lock concealment preventing direct attack.**
- **No externally visible weak points.**

6. DST Certification Process (DST Certified™)

To be recognised as DST Certified™, a product must undergo and pass a five-stage evaluation:

Stage 1 — Documentation Review

- **Engineering drawings**
- **Design intent**
- **Material specifications**
- **Installation environment**

Stage 2 — Disguise Validation

- **In-situ assessment**
- **Observation tests by non-technical participants**
- **Multi-angle recognition analysis**

Stage 3 — Security Testing

Conducted by an approved test authority such as BRE/LPCB or Sold Secure:

- **Forced-entry simulations**
- **Tamper and attack resistance**
- **Structural stress testing**
- **Environmental exposure testing**

Stage 4 — Installation Assessment

- **Fixing integrity**
- **Mounting strength**
- **Incorrect installation risk evaluation**

Stage 5 — Certification & Registration

Products passing all requirements receive:

- **DST Certified™ designation**
- **Certificate of compliance**
- **Registration in the DST Product Register**
- **Eligibility for DST licensing and authorised branding**

7. Exclusions

DST certification explicitly excludes:

- **Visible key safes**
- **Painted or cosmetic disguises**
- **Decorative covers**
- **Traditional lockboxes**
- **Products with exposed mechanisms**
- **Devices relying solely on deterrence through visibility**

Only products engineered for true concealment + security qualify.

8. Governance & Ownership

DST Standard v1.1 is authored and governed by:

KeySpot Security Ltd
Founder: Mark Cowie
Role: Originator of the Disguised Security Technology™ category
Custodian of the DST Certified™ mark

Future revisions will be developed in collaboration with:

- **Academic institutions**
- **Security testing houses**
- **Insurance bodies**
- **Police and regulatory partners**
- **Industry experts**

9. Future Development Pathway

Projected expansions include:

- **DST Standard v2.0 — International harmonisation**
- **DST Standard v3.0 — Full insurance integration model**

- **DST Smart Device Standard — Emerging digital/IoT disguised security**
- **DST Product Family Standards — Housing, commercial, and industry-specific DST categories**

10. Summary Statement

Disguised Security Technology™ establishes a new global category of security engineering wherein concealment is a functional protective feature. This standard sets the foundational design, performance, testing, and compliance expectations required to classify and certify disguised security products under the DST Certified™ framework.