

FR-IMG-005 — Image Verification

[Go to Crucible Image Management Requirements](#)

Statement

[Crucible](#) SHALL verify the [Digital Signature](#) associated with an identified [Image](#).

Derived From

This requirement derives from:

- Crucible System Requirements Specification, Version 1.1 Draft, Functional Requirements, FR-IMG-005

The Original Requirement states:

[Crucible](#) SHALL perform [Digital Signature Verification](#) for the [Digital Signature](#) associated with an identified [Image](#).^[C1]

FR-IMG-005 replaces the phrase **perform Digital Signature Verification for** with the direct verb **verify** while preserving the subject of the verification and its association with the identified Image.

No other substantive normalization is required.

Rationale

[Digital Signature Verification](#) determines whether a [Digital Signature](#) is valid for an identified [Image](#) under the applicable verification conditions.

Verification can identify whether:

- The Image differs from the signed representation
- The Digital Signature does not correspond to the identified Image
- The Digital Signature is invalid
- The signing identity does not satisfy the applicable trust conditions

A valid Digital Signature does not independently establish that the Image:

- Is free from vulnerabilities
- Satisfies a compliance baseline
- Is approved for promotion
- Is authorized for deployment
- Is compatible with a target platform

- Is suitable for a specified purpose

Separate requirements govern those determinations.

Applies To

This requirement applies to:

- [Crucible](#)
- [Digital Signature Verification](#)
- [Digital Signatures](#)
- [Images](#)

Verification

Verification confirms that:

1. An identified [Image](#) with an associated [Digital Signature](#) is selected for verification
2. [Crucible](#) verifies the associated Digital Signature
3. Crucible determines whether the Digital Signature is valid for the identified Image
4. Crucible produces a verification result

Referenced By

The following pages reference this requirement:

- [5.2 Construct Images](#)
- [6.1 Construct and Assess the Environment](#)
- [Annex D: Requirements Traceability](#)

Implementation Status

Implemented and Verified

Requirement Status

☐ Review and approve FR-IMG-005 as a leaf requirement.

Issues

- ☐ Determine whether separate requirements define the applicable trust conditions and trusted signing identities.
- ☐ Determine whether separate requirements govern preservation of the Digital Signature Verification result.

Notes for Editors

This requirement page retains the stable requirement identifier FR-IMG-005.

This page is a leaf requirement page and omits a trailing `:start` from its namespace.

The Statement preserves the approved source intent by requiring Crucible to verify the Digital Signature associated with an identified Image.

Do not add vulnerability scanning, compliance assessment, Image approval, promotion, publication, transfer, deployment validation, signature-algorithm, trust-store, or key-governance obligations unless the controlling requirement changes through an approved requirements process.

To reference this requirement Statement from another wiki page, insert:

```
{{section>dido:02-crusible:99-annexes:annex-c-requirements:03-functional-requirements:03-02-image-management:fr-img-005#Statement&noheader&nofooter&noeditbtn}}
```

© 2026 Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

From:
<https://wiki.didosolutions.com/> - Dido Solutions, Inc Wiki

Permanent link:
<https://wiki.didosolutions.com/dido/02-crusible/99-annexes/annex-c-requirements/03-functional-requirements/03-02-image-management/fr-img-005>

Last update: 2026/07/30 05:41

