FR-IMG-005 — Image Verification

Go to Crucible Image Management Requirements

Statement

Crucible SHALL verify the digital signature associated with an identified Image.

Source Statement

> Crucible SHALL perform Digital Signature Verification for the Digital Signature associated with an identified Image.

Source

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

Assessment

The source statement expresses the approved intent but does not provide a fully testable formulation.

The following Specification Discipline and Authoring findings apply:

- **The system** does not use the defined system name
- **shall** does not follow the established uppercase normative convention
- **Support** is a weak verb that does not identify the required behavior
- **Image verification** does not identify what property of the Image is verified
- The source statement does not identify the observable result of verification
- The source statement does not prescribe a signature algorithm, trust store, certificate mechanism, key-management system, or implementation technology

Within the surrounding Image Management requirements, FR-IMG-004 establishes Image signing. FR-IMG-005 therefore treats verification as verification of the digital signature associated with an identified Image.

The normalized Statement:

- Replaces **The system** with Crucible
- Replaces **support** with the direct behavior **verify**
- Identifies the digital signature as the subject of verification
- Identifies the Image associated with the signature
- Retains one primary required behavior
- Preserves implementation independence

The normalized Statement does not independently require vulnerability scanning, compliance assessment, functional testing, Image approval, promotion, or deployment validation.

Rationale

Verification of the digital signature associated with an identified Image allows Crucible to determine whether the signature remains valid for the evaluated Image under the applicable verification conditions.

Signature verification can detect:

- Modification of signed Image content
- A mismatch between an Image and its signature
- An invalid signature
- An unrecognized signing identity
- A signing identity that does not satisfy the applicable trust conditions

Image verification contributes to:

- Image integrity evaluation
- Image authenticity evaluation
- Controlled Image promotion
- Controlled Image distribution
- Controlled Image deployment
- Auditability
- Evidence
- Traceability

A valid digital signature does not by itself 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
- Images
- Machine Images
- Container Images
- Image identifiers

- Image content digests
- Digital signatures
- Signing identities
- Verification conditions
- Verification operations
- Image repositories
- Image promotion workflows
- CI/CD Pipelines

Verification

1. Verification SHALL confirm that Crucible evaluates the digital signature associated with an identified Image
2. Verification SHALL confirm that Crucible determines whether the evaluated digital signature is valid for the identified Image
3. Verification SHALL confirm that Crucible records the verification result

Verification may include:

- Valid-signature testing
- Invalid-signature testing
- Modified-Image testing
- Image-and-signature mismatch testing
- Unrecognized-signing-identity testing
- Signature-record inspection
- Image-digest comparison
- Verification-log inspection
- Automated CI/CD Pipeline testing

The verification record SHALL identify:

1. The evaluated Image
2. The Image identifier
3. The evaluated digital signature
4. The applicable verification conditions
5. The verification operation
6. The verification result
7. The observed output
8. The generated Evidence

Outgoing Traceability

This requirement realizes:

- MO-001
- MO-005
- MO-006

This requirement relates to:

- FR-IMG-001 — Build Virtual Machine Images
- FR-IMG-002 — Build Container Images
- FR-IMG-004 — Image Signing
- FR-IMG-006 — Image Promotion Workflows
- FR-DEP-007 — Deployment Validation
- 6. Machine Images and Image Layers
- 9. Compliance and Security
- 10. Reproducibility, Provenance, and Traceability

Referenced By

The wiki Backlinks function provides the current list of pages that reference `FR-IMG-005`.

Incoming Traceability should be derived dynamically from backlinks rather than maintained as a duplicate manual list.

Backlinks identify incoming references but do not define the semantics of each relationship. Referencing pages should identify whether the relationship represents realization, refinement, verification, dependency, or another defined traceability relationship.

ConOps Relationship

The Crucible Concept of Operations describes a Phase 1 workflow that builds and processes controlled Image Artifacts through an automated CI/CD Pipeline.

FR-IMG-005 establishes the required digital-signature verification behavior for an identified Image processed by that workflow.

Requirements governing Image building, signing, compliance assessment, promotion, publication, transfer, and deployment define separate behavior.

Delivery Phase

Phase 1

Implementation Status

Not Assessed

Implementation status requires verification that Crucible verifies the digital signature associated with an identified Image.

Requirement Status

Draft

The source System Requirements Specification identifies Version 1.1 as a draft.

Notes for Editors

This requirement page should retain the stable requirement identifier `FR-IMG-005`.

Changes to the Statement SHALL preserve the approved intent of the source requirement.

The Source Statement should preserve the original wording from the controlling System Requirements Specification.

The Statement should remain limited to verification of the digital signature associated with an identified Image.

Requirements for vulnerability scanning, compliance assessment, Image approval, promotion, publication, transfer, and deployment validation should remain in their applicable requirement pages.

Verification criteria should test only the behavior stated in the normalized Statement and should not introduce additional normative obligations.

Incoming Traceability should use the wiki Backlinks function rather than a manually maintained list.

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}}
```

Do not rename this page after an external citation unless a redirect or move plan is in place.

© 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?rev=1784563114

Last update: **2026/07/20 08:58**