NOD-003e — Protect Sensitive Configuration Values

Go to NOD-003 — Configure a Node

Statement

The DIDO-TE SHALL protect each Sensitive Configuration Value throughout its Lifecycle.

Derived From

- NOD-003 — Configure a Node
- NOD-003a — Select the Node Configuration
- NOD-003b — Resolve Node Configuration Values
- NOD-003c — Apply the Node Configuration
- NOD-003d — Establish Node Bindings
- [DTE5] DIDO-TE Requirements Register, source requirement identifier and obligation to be assigned
- [DTE6] Structured Information Processing Reference Architecture (SIP-RA)
- [DTE7] Federated Data Interpretation Systems Reference Architecture (FDIS-RA)

Rationale

A Node Configuration may contain Credentials, Cryptographic Material, authentication tokens, personal information, network details, proprietary values, or other Information whose disclosure, alteration, substitution, or misuse may compromise a Node or Test Environment.

Protection applies while a Sensitive Configuration Value is created, obtained, transferred, stored, resolved, applied, used, recorded, retained, and disposed of. The applicable Security Controls depend upon the value's Classification and the risks associated with unauthorized access or modification.

A protected reference, Identifier, digest, or redacted representation may preserve Evidence and Traceability without exposing the Sensitive Configuration Value.

This requirement governs the protection of Sensitive Configuration Values. It does not require the DIDO-TE to reproduce secret values in Configuration Records, logs, Test Results, or Evidence.

Applies To

- DIDO-TE
- Node
- Node Configuration

- Configuration Value
- Sensitive Configuration Value
- Configuration Source
- Configuration Record
- Credential
- Cryptographic Material
- Test Environment
- Test Execution
- Evidence
- Traceability

Verification

Verification confirms that:

- The DIDO-TE identifies each Configuration Value requiring protection.
- Each Sensitive Configuration Value has an applicable Classification and handling rule.
- The applicable Security Controls address Confidentiality, Integrity, availability, Access Control, use, transfer, storage, retention, and disposal.
- Only identified and authorised actors, Nodes, processes, and services have access to a Sensitive Configuration Value.
- Access remains limited to the Sensitive Configuration Value and operation required by the authorised activity.
- The DIDO-TE protects Sensitive Configuration Values during storage and transfer.
- The DIDO-TE protects Sensitive Configuration Values from unauthorised disclosure, alteration, substitution, duplication, extraction, and reuse.
- The DIDO-TE prevents Sensitive Configuration Values from appearing in unprotected configuration files, command histories, process arguments, logs, error messages, Test Results, or Evidence.
- The DIDO-TE uses protected references, Identifiers, digests, or redacted representations when records require identification without disclosure.
- Protection does not prevent verification of the Sensitive Configuration Value’s identity, source, authority, integrity, applicability, or use.
- The DIDO-TE detects an expired, revoked, altered, substituted, exposed, or unauthorised Sensitive Configuration Value.
- The DIDO-TE prevents use of a Sensitive Configuration Value that fails an applicable validity or protection criterion.
- The DIDO-TE records access to and material use of Sensitive Configuration Values without recording the exposed values.
- The DIDO-TE rotates, revokes, replaces, archives, or disposes of Sensitive Configuration Values in accordance with applicable Security Controls.
- A change to a Sensitive Configuration Value produces a distinguishable configuration revision and triggers applicable Configuration Validation.
- The DIDO-TE maintains Traceability among the Sensitive Configuration Value, its Classification, protected reference, authorised Configuration Source, authorised users, Node Configuration, Node instance, Security Controls, access records, findings, exceptions, and resulting Evidence.
- A missing, exposed, altered, unprotected, unauthorised, improperly retained, or untraceable Sensitive Configuration Value constitutes nonconformance with this requirement.

Verification includes:

- Inspection of Sensitive Configuration Value identification and Classification
- Inspection of applicable handling rules and Security Controls
- Inspection of Access Control assignments
- Inspection of storage and transfer protections
- Inspection of configuration files, command histories, process arguments, logs, error messages, Test Results, and Evidence for exposed values
- Confirmation that protected references preserve identity and Traceability without disclosing Sensitive Configuration Values
- A negative assessment involving unauthorised access
- A negative assessment involving an altered, expired, or revoked Sensitive Configuration Value
- A negative assessment involving attempted disclosure through a log or error message
- Confirmation that an invalid Sensitive Configuration Value prevents the applicable configuration or execution activity
- Inspection of access, rotation, revocation, retention, and disposal records
- Inspection of findings, exceptions, Evidence, and Traceability

Referenced By

Plugin Backlinks: Nothing was found.

Related Architecture Sections

- Add links to the architecture sections governing Sensitive Configuration Values, Information Classification, Access Control, cryptographic protection, Credential management, logging, retention, disposal, Evidence, and Traceability.

Delivery Phase

Assign the applicable delivery phase.

Requirement Status

Draft

Statement Reference

Use the following syntax to reference this requirement’s Statement section from another DokuWiki page:

```
{{section>dido:03-dido-te:99-annexes:annex-c-requirements:03-node-requirements:nod-003-configure-a-node:nod-003e-protect-sensitive-configuration-values#Statement&noheader&nofooter&noeditbtn}}
```