

GPR-021 — Security Analysis

[Go to Annex C: Requirements](#)

Statement

The Submission SHALL provide a security analysis identifying the security-sensitive elements introduced by the proposed specification, the applicable security-policy controls, the required security awareness, the recommended default security policies, and the security considerations applicable to implementers.

Requirement Level

Mandatory

Rationale

A security analysis makes the security implications of the proposed specification explicit and allows reviewers, implementers, operators, and responsible authorities to determine whether appropriate protections can be applied.

Identifying security-sensitive elements, controlled forms of access, security-aware components, default policies, and implementation considerations reduces the risk that security requirements remain implicit or are applied inconsistently.

Required Analysis

The security analysis addresses:

1. Security-sensitive elements introduced by the proposed specification
2. Forms of access to those elements that should be subject to security-policy control
3. Services, facilities, or architectural elements that need to be security-aware
4. Recommended default policies for authentication, auditing, authorization, message protection, and other applicable controls
5. Security considerations that implementers need to understand and address
6. Security assumptions, dependencies, limitations, and residual risks

Evaluation Criteria

A conforming Submission demonstrates that:

1. Each security-sensitive element is identified or the absence of such elements is explicitly stated and justified
2. Access requiring security-policy control is identified
3. Security-aware services, facilities, and architectural elements are identified
4. Recommended default security policies are described
5. Security considerations relevant to implementation and deployment are documented
6. Security assumptions, dependencies, limitations, and residual risks are disclosed
7. The analysis supports the secure-implementation demonstration required by GPR-020

Referenced By

- [5.1.11 Security](#)

Related Requirements

1. [GPR-020 — Secure Implementation and Deployment](#)
2. [SIP-017 — Cross-Security-Boundary Integration](#)
3. [SIP-018 — Information-Flow Segmentation](#)

Notes for Editors

The Required Analysis section elaborates the required coverage of this requirement. Its entries are not independently numbered requirements.

A Submission may determine that the proposed specification introduces no security-sensitive elements. In that case, the Submission must state that conclusion and provide its supporting analysis.

OMG security specifications identified by references [SEC] and [RAD] may provide useful resources for preparing this analysis.

To transclude the authoritative Statement into another page, use:

```
{{section>public:00-sip-ra:99-annexes:annex-c-requirements:gpr-021-security-analysis#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/public/00-sip-ra/99-annexes/annex-c-requirements/gpr-021-security-analysis>

Last update: 2026/09/15 13:41



