SWIM-SERV-013 Access and use conditions

Requirement

Title	Service access and use conditions
Identifier	SWIM-SERV-013
Requirement	A service description **shall** include the conditions which apply to accessing and using the service, such as • legal constraint; • service policies; • service consumption constraints; and • security constraints.
Rationale	This requirement ensures that a service consumer is aware of any limitations on the access and use of the service. It is good practice to share business constraint information associated with the conditions of usage of the service.
Verification	Completeness: Verify that the elements included cover the required constraints and policies. Consistency: Not Applicable. Correctness: Not Applicable.

Examples /Notes	Example legal constraints:
	
	• Licenses to be bought;
	• Intellectual property rights to be respected.
	
	Example services policies:
	
	• Contingency policy;
	• Business policy(s) in terms of business rule or objective i.e. how the business is conducted;
	• Operational policy(s) (i.e. constraints and requirements for how services operate and interoperate at runtime) in terms of rules and guidelines. Operational policies are utility centric (handling operational characteristics) covering mainly; , logging, messaging protocol and versioning. Normally standardised for a defined collection of services;
	• Technical policy(s). Technical policies can (if available) be provided in machine-readable format;
	• Versioning scheme used (e.g. major.minor[.fix]) and the compatibility guaranteed between different versions (e.g. backwards compatibility is guaranteed between minor versions but not for major);
	• Lifecycle policy applied to the service (e.g. to allow consumers to know that he is not investing on a soon to be retired service).
	
	Example service consumption constraints:
	
	• The maximum number of requests per time window allowed for a service consumer.
	
	Example security constraints:
	
	• Confidentiality:
	  • Statement of the confidentiality offered by the service (e.g. message, transport, none…);
	  • Elements of the payload whose confidentiality is required or provided (whole payload, body, specific sub-elements…);
	  • Cryptographic algorithms and key sizes;
	• Integrity:
	  • Statement of the integrity offered by the service (e.g. message, transport…);
	  • Elements of the payload whose integrity is required or provided (whole payload, body, specific sub-elements…);
	  • Cryptographic algorithms and key sizes;
	• Authentication:
	  • Statement of the authentication mechanisms used on consumer and provider side;
	  • Statement of the failed authentication constraints;
	  • Identity tokens;
	• Authorisation:
	  • Statement on the authorisation mechanism used;
	  • Credentials used for the authorisation;
	  • Levels of authorisation.
	
	Note: Additional use conditions could be diplomatic, geographical reasons, safety criticality and fees to be paid, for instance.

Level of Implementation	Mandatory

Guidance

No guidance provided.

Guidance for JSON service description

> ⓘ **tentative JSON Guidance**
>
> Guidance for JSON service descriptions integrated within the SWIM Service Description Handbook.

Schema

The guidance concerns JSON Schema v0.0.3 (see Schema releases).

```
                  "ServiceGeneralDescription" :
                  {
                          "description" : "Description of the service in terms of what it provides, the
purpose and under which conditions and quality levels the service is provided.",
                          "type": "object",
                          "additionalProperties": false,
                          "required": ["operationalNeed", "functionality", "qualityOfService",
"accessAndUseCondition", "validation"],
                          "properties":
                          {

                                  "accessAndUseCondition":
                                  {
                                          "description" : "A condition which applies to accessing and
using the service, such as legal constraint, service policies, service consumption constraints and
security constraints. [SWIM-SERV-013]",
                                          "type" : "array",
                                          "items" : { "$ref":"#/definitions/AccessAndUseCondition" },
                                          "minItems": 1
                                  }

                          }
                  }


                  "AccessAndUseCondition" :
                  {
                          "description" : "A condition which applies to accessing and using the service,
such as legal constraint, service policies, service consumption constraints and security constraints.
[SWIM-SERV-011]",
                          "type": "object",
                          "additionalProperties": false,
                          "required": ["description"],
                          "properties":
                          {
                                  "description":
                                  {
                                          "description" : "Description of the conditions that influence
accessing and using the service, such as legal constraint; service policies; service consumption
constraints (SWIM-SERV-013). Concrete access control and other security mechanisms are described in the
technical section of the form.",
                                          "type" : "string",
                                          "minLength":1
                                  },
                                  "name":
                                  {
                                          "description" : "The name of the condition.",
                                          "type" : "string"
                                  },
                                  "type":
                                  {
                                          "description" : "The type of service access or use condition.
[SWIM-SERV-013]",
                                          "$ref" : "#/definitions/CodeAccessAndUseConditionType"
                                  }
                          }
                  }
```

```
"CodeAccessAndUseConditionType" :
{
        "description" : "A code listing access and use conditions.",
        "type": "string",
        "enum":
        [
                "LEGAL_CONSTRAINT",
                "OTHER",
                "SECURITY_CONSTRAINT",
                "SERVICE_CONSUMPTION_CONSTRAINT",
                "SERVICE_POLICY"
        ]
}
```

Rules expressed for the cases as defined in Registry URD.

case	rules
COMPLIANT	mandatory
CANDIDATE	
DEFINITION	

Guidance

List the conditions that apply to access or use the service, so that a service consumer is aware of any limitations on the access and use of the service.

Within field accessAndUseCondition, itself within field serviceGeneralDescription, list **one or more** occurrences of type AccessAndUseCondition.

AccessAndUseCondition - Mandatory

A condition which applies to accessing and using the service, such as legal constraint, service policies, service consumption constraints and security constraints.

Example legal constraints:

- Licenses to be bought;
- Intellectual property rights to be respected.

Example services policies:

- Contingency policy;
- Business policy(s) in terms of business rule or objective i.e. how the business is conducted;
- Operational policy(s) (i.e. constraints and requirements for how services operate and interoperate at runtime) in terms of rules and guidelines. Operational policies are utility centric (handling operational characteristics) covering mainly; , logging, messaging protocol and versioning. Normally standardised for a defined collection of services;
- Technical policy(s). Technical policies can (if available) be provided in machine-readable format;
- Versioning scheme used (e.g. major.minor[.fix]) and the compatibility guaranteed between different versions (e.g. backwards compatibility is guaranteed between minor versions but not for major);
- Lifecycle policy applied to the service (e.g. to allow consumers to know that he is not investing on a soon to be retired service).

Example service consumption constraints:

- The maximum number of requests per time window allowed for a service consumer.

Example security constraints:

- Confidentiality:
    - Statement of the confidentiality offered by the service (e.g. message, transport, none…);
    - Elements of the payload whose confidentiality is required or provided (whole payload, body, specific sub-elements…);
    - Cryptographic algorithms and key sizes;
- Integrity:
    - Statement of the integrity offered by the service (e.g. message, transport…);
    - Elements of the payload whose integrity is required or provided (whole payload, body, specific sub-elements…);
    - Cryptographic algorithms and key sizes;
- Authentication:
    - Statement of the authentication mechanisms used on consumer and provider side;
    - Statement of the failed authentication constraints;
    - Identity tokens;
- Authorisation:

- Statement on the authorisation mechanism used;
- Credentials used for the authorisation;
- Levels of authorisation.

Note: Additional use conditions could be diplomatic, geographical reasons, safety criticality and fees to be paid, for instance.

> ℹ️ **note**
>
> Concrete access control and other security mechanisms are described in the technical section of the form (see SWIM-SERV-019 Protocols and data format)

attribute name	description	type		guidance	rule
type	The type of service access or use condition. [SWIM-SERV-013]	A code listing the types of access and use conditions.		Select the code value indicating the type of condition	Mandatory
		LEGAL_CONSTRAINT	Eg Licenses to be bought, Intellectual property rights to be respected.		
		SERVICE_POLICY	A constraint governing one or more services. Eg Contingency policy, Business policy, Operational policy, Technical policy(s), Versioning scheme, Lifecycle policy		
		SERVICE_CONSUMPTION_CONSTRAINT	Eg The maximum number of requests per time window allowed for a service consumer.		
		SECURITY_CONSTRAINT	Eg Confidentiality, Integrity, Authentication, Authorisation		
		OTHER	eg diplomatic, geographical reasons, safety criticality or fees to be paid		
name	The name of the condition.	string		Provide a short name for the condition.	Mandatory
description	Description of the conditions that influence accessing and using the service, such as legal constraint; service policies; service consumption constraints	string		Describe the conditions which apply to accessing and using the service, so that the consumer is aware of any limitations on the access and use of the service.	Mandatory

Policy document - Optional

Additional information may be provided as a document of type POLICY_DOCUMENT.

See Guidance on serviceDocument on how to fill in documents.

Example

```
                "serviceGeneralDescription": {

                        "accessAndUseCondition": [
                                {
                                        "type": "SECURITY_CONSTRAINT",
                                        "name": "User id + password",
                                        "description": "The access to the service is based on user id and
password."
                                },
                                {
                                        "type": "SECURITY_CONSTRAINT",
                                        "name": "SLA",
                                        "description": "The access to the service is subject to the
signature of a Service Level Agreement with the Donlon Airport Operator."
                                }
                        ]

                }
```

A complete JSON example is available in page JSON example - Donlon TOBT Setting service description.