
# TDH022 – TECHNICAL INTEROPERABILITY GUIDELINES AND API MANAGEMENT

## Operative Document

## Interaction Patterns

Versione: 0.2

Data: 22/22/2022

| Version | Release Date | Release Type |
|---|---|---|
| 0.1 | 17/12/2021 | First Release – Italian |
| 0.2 | 22/02/2022 | Second Release – English |

## *Contents Index*

# CHAPTER 1 – INTRODUCTION

This Operative Document identifies the combinations of Interaction Patterns *(indicated in this document) and Security Patterns (indicated in the Operative Document - Security Patterns),* which solve the needs related to communication activities between users *(in this sense we consider all subjects that use the digital services made available by providers within the Ecosystem)* certified within the Tourism Digital Hub and providers *(in this sense we consider Public Institutions such as, for example, Regions and Provinces, as well as Public Entities or similar and Private Entities, including Second and Third Parties that make services and functionalities available to the TDH)* also certified within the Tourism Digital Hub, as an example, Regions and Provinces, as well as Public Entities or similar and Private Entities, including Second and Third Parties that make services and functions available to the TDH also certified to the Tourism Digital Hub.

Interoperability profiles are chosen by providers according to specific application needs in relation to the nature of the users.

This document, the application of which relates to the specific context of the Tourism Digital Hub (TDH), follows the provisions of the Operational Document "Interoperability Profiles"[1] issued by AgID and linked to the document " Guidelines on Technical Interoperability of Public Administrations"[2] also issued by AgID; in addition to the above, please refer to the two documents mentioned above for detailed indications

[1] Online Reference: https://www.agid.gov.it/sites/default/files/repository_files/03_profili_di_interoperabilita.pdf
[2] Online Reference: https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf

# CHAPTER 2 – APPLICATION SCOPE

This Operative Document is drafted as an operational document related to the Guideline on technical interoperability to be followed on both the user and provider sides for the purposes of certification to the Tourism Digital Hub.

### *2.1 Recipients of this document*

This Operative Document is intended for all providers who provide users with services and functions within the Tourism Digital Hub (TDH), as well as for the users themselves, in order to enable the fruition of the desired services and functions; therefore, these provisions can be used as a basis for the implementation of new functions in case they have to be developed from scratch or as a basis for the integration of existing functions.

The following is a list of Public and Private Parties to whom the Operational Document is addressed, both as providers and users of services and functions within the Tourism Digital Hub (TDH).

*Public Parties*

- Central Public Administration (e.g., Ministry of Tourism),
- Local Public Administration (e.g., Regions, Provinces...),
- National and Local Authorities (e.g., ENIT),
- Non-Profit Organizations,
- Public Enterprises related to tourism (e.g., ski lifts...).

*Private Parties*

- Hospitality enterprises, catering enterprises, etc.,
- Tour Operators/Travel Agencies,
- Unions,
- Private Enterprises related to tourism (e.g., ski lifts…).

# CHAPTER 3 – REFERENCES AND ABBREVIATIONS

## *3.1 Document Reading Notes*

In accordance with ISO/IEC Directives, Part 3 for drafting technical documents this Operational Document will use the keywords "MUST", "MUST NOT", "SHOULD", "SHALL NOT", "MAY" and "OPTIONAL", the interpretation of which is described below:

- **MUST**, specify a mandatory requirement to comply with Guidelines;
- **MUST NOT**, indicate an absolute no-go on specifications;
- **SHOULD or SHOULD NOT**, mean that the implications must be understood and carefully weighed before choosing alternative approaches;
- **MAY or OPTIONAL**, signifies that the reader may choose to apply or not apply the specification without any kind of implication or restriction.

## *3.2 Terms and Definitions* [3]

For an easier reading, a glossary of terms and definitions contained in this document is given below.

| | |
|---|---|
| **[AgID]** | Digital Agency for Italy |
| **[CAD]** | Legislative Decree 7 March 2005, n. 82 - "Digital Administration Code" (also known as "CAD"), updated with amendments by Legislative Decree 76 of 16 July 2020 and converted into law with Law 120 of 11 September 2020 |
| **[Provider]** | One of the subjects referred in Article 2, paragraph 2 of the CAD that makes e-services available to other organizations, for the use of data in its possession or the integration of the processes it has carried out |

[3] Some terms and definitions explained in this paragraph are also available in the Guidelines on Technical Interoperability for Public Administrations issued by AgID (see the section "Reference Bibliography and Sitography" for the redirect links to the cited contents).

| | |
|---|---|
| **[User]** | Organization that uses the e-services made available by one of the subjects referred in Article 2, paragraph 2 of the CAD |
| **[REST]** | Representational State Transfer |
| **[RPC]** | Remote Procedure Call |
| **[SOAP]** | Simple Object Access Protocol |
| **[TDH]** | Tourism Digital Hub |
| **[TDH022]** | TDH022 - Interoperability interface of the Tourism Digital Hub |
| **[Trust]** | One of the most important means of managing security issues in the exchange of information in the network to enable interoperability between systems. It is based on mutual recognition of interacting entities and trust in each other's behavior |
| **[UML]** | Unified Modeling Language |

### *3.3 Reference Standards*[4]

The following are the technical standards that are essential for the application of this document.

| | |
|---|---|
| **[X.509]** | International Telecommunication Union (ITU-T) standard, which defines the format of public key certificates and certificate authorities |

[4] Some terms and definitions explained in this paragraph are also available in the Guidelines on Technical Interoperability for Public Administrations issued by AgID (see the section "Reference Bibliography and Sitography" for the redirect links to the cited contents).

# CHAPTER 4 – INTEROPERABILITY PROFILES

*The content of this chapter highlights what is reported in Chapter 4 of the " Operative Document: Interoperability Profiles" published by AgID, to which reference should be made for the detailed explanation of the flow of interactions, while here we report only the general contents, always following what is reported in Chapter 4 of the above-mentioned document.*

### *4.1 User confidentiality and authentication profile*

In order to implement the choice of interoperability profiles, it is necessary to follow an exchange between user and provider (both certified within the TDH), so as to guarantee

- Confidentiality at the channel level (in terms of protecting information against unauthorized or accidental access),
- Authentication of the user.

In this sense, the user may not coincide with the user organizational unit but may in any case belong to it.

The profile of confidentiality and authentication of the user is not strictly related to the implemented Interaction Pattern (in this sense it is independent) and uses certain security patterns such as:

- ID_AUTH_CHANNEL_01
- ID_AUTH_SOAP_01 or ID_AUTH_REST_01

It also assumes the existence of a trust between user and provider that establishes:

- Recognition, by the provider, of X.509 certificates or the issuing CA, related to the user,
- The recognition by the user of the X.509 certificate or the issuing CA relating to the provider.

*The mechanisms by which the trust is established do not affect the flow of interactions related to this Profile; please refer to Chapter 4.1 of the " Operative Document related to the Interoperability Profiles" published by AgID for a detailed explanation of the underlying flow of interactions (please refer to the section "Reference Bibliography and Sitography" for redirect links to the cited contents).*

### *4.2 Non-repudiation transmission solutions*

It is necessary to follow up an exchange between the user and the provider that guarantees the non-repudiation of the transmission *(understood as a guarantee that the parties involved in a given exchange cannot deny having taken part in it)*[5] ensuring at the message level:

- message integrity,
- authentication of the user, as an organization or organizational unit user as the sender of the content,
- confirmation by the provider of the receipt of the content,
- opposability to third parties,
- robustness of transmission.

This interoperability profile uses the BLOCK_SOAP Interaction Pattern in case of SOAP use or BLOCK_REST in case of REST use. In this sense, the following Security Patterns are used:

- ID_AUTH_CHANNEL_01 or, alternatively, ID_AUTH_CHANNEL_02,
- **for SOAP**: ID_AUTH_SOAP_02 and INTEGRITY_SOAP_01,
- **for REST**: ID_AUTH_REST_02 and INTEGRITY_REST_01.

We assume the existence of a trust between user and provider within the TDH, which states:

- that there is mutual recognition by the issuer and the user of X.509 certificates, or issuing CAs,
- that the mechanism by which the trust is established does not condition what is described in this section. The user and the issuer must agree to this:
    - a unique identifier of the message, necessary to guarantee the detection of retransmissions (see ID_AUTH_SOAP_02 and ID_AUTH_REST_02), and the related exchange modalities
    - the persistence time frame of the messages which depends on the characteristics of the content of the exchanged data and in compliance with legal regulations
    - the transaction validity time between:
        - the instant of forwarding by the user,
        - the instant of reception by the dispenser;

[5] The underlying need, in this sense, is functional to the use of digital signatures, based on cryptographic algorithms

- the maximum time the user has to wait for the reply message to be considered as not having taken place;
- the maximum number of return attempts by the user accepted by the provider;
- possible use of alternative channels to overcome or highlight communication problems encountered.

Through encryption technologies, the following properties are guaranteed:

- integrity and non-repudiation of the message sent by the user,
- integrity and non-repudiation of the confirmation message from the provider,
- authentication of the user,
- authentication of the provider,
- temporal validation that certifies the instant in which the message was transmitted,
- temporal validation certifying the instant in which the message was received.

Please refer to Chapter 4.2 of the " Operative Document related to Interoperability Profiles" published by AgID for a detailed analysis of the flow of interactions below (please refer to the section "Bibliography and Sitography of Reference" for redirect links to the contents mentioned).

# REFERENCE BIBLIOGRAPHY AND SITOGRAPHY

**Guidelines on Technical Interoperability of Public Administrations**

Author: AgID – First Release: 27/04/2021

Online reference: https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf

**Operative Document – Interoperability Profile**

Author: AgID – First Release: 27/04/2021

Online reference: https://www.agid.gov.it/sites/default/files/repository_files/03_profili_di_interoperabilita.pdf