TDH022 – TECHNICAL INTEROPERABILITY GUIDELINES AND API MANAGEMENT

Operative Document

Security Patterns

Versione: 0.2

Data: 22/02/2022

Version	Release Date	Release Type
0.1	21/12/2021	First Release – Italian
0.2	22/02/2022	Second Release – English

Contents Index

CHAPTER 1 – INTRODUCTION

This Operative Document describes the security patterns in communication that providers *(in this sense we consider Public Institutions such as, by way of 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)* certified within the Tourism Digital Hub must use them to satisfy the needs identified by functional and non-functional requirements concerning specific interactions with the relative users, also certified within the Tourism Digital Hub *(in this sense we consider all subjects that use the digital services made available by the providers within the Ecosystem).* The security patterns described in this Operational Document follow what is indicated in the Operational Document "Security Patterns" issued by AgID and linked to the document "Guidelines on technical interoperability of Public Administrations" also issued by AgID; in addition to what is reported, please refer to the two documents mentioned above for detailed indications.

1.1 Security Pattern: Preliminary Information

Security Patterns, from a general point of view, cover the security aspects of communication between the domains of the single parties; these parties maintain their autonomy in the organizational and security aspects within their own domain; here is some general information on the subject:

- Define, at the level of technological specification, a "shared tool" useful to promote interoperability between providers and users;
- Provide a common language for users and providers to address the needs and characteristics of service interfaces;
- Provide developers with technical methods supported by documented, reviewed and tested technology standards to expose digital services.

Finally, it is necessary to emphasize the purpose of these patterns, that is to define how to ensure that the interactions between user and provider (both certified within the Tourism Digital Hub) are made in accordance with the specific security requirements determined by the nature of the

interchange of data, information, content and the like made and the regulatory requirements that have determined them.

The implementation of Security Patterns is closely related to that of Interaction Patterns (to which they apply) and their implementation methods at the practical level are chosen by the provider according to the specific application needs of the technical level of users.

Given the constant evolution of the technological context, the list of Security Patterns is constantly updated and can be consulted in the AgID Documentation (see Chapter 7 of the document "Guidelines on Technical Interoperability of Public Administrations" for detailed information).

CHAPTER 2 – APPLICATION SCOPE

This Operative Document is intended to be an operative document related to the Technical Interoperability Guideline for security aspects.

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 Definition [1]

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

[1] 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

CHAPTER 4 – CHANNEL SECURITY AND/OR ORGANIZATION IDENTIFICATION

The content of this chapter highlights what is reported in Chapter 4 of the " Operative Document: Security Pattern" published by AgID, to which we refer for the detailed explanation of the processing rules, while here we report only the general contents, always following what is reported in Chapter 4 of the above-mentioned document (please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).

4.1 [ID_AUTH_CHANNEL_01] Direct Trust Transport-Level Security

Concerning the communication between user and provider that ensures, at channel level:

- confidentiality;
- integrity;
- Identification of the provider as an organization;
- defense against threats deriving from attacks: Replay Attack and Spoofing.

Please refer to Chapter 4.1 of the Operative Document related to Security Patterns published by AgID for a detailed description of the above-mentioned Patterns and of the related underlying processing rules *(please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).*

4.2 [ID_AUTH_CHANNEL_02] Direct Trust mutual Transport-Level Security

Concerning the communication between user and provider that ensures, at channel level:

- confidentiality;
- integrity;
- Identification of the provider and the user as an organization;
- defense against threats from attacks: Replay Attack and Spoofing.

Please refer to Chapter 4.2 of the Operative Document related to Security Patterns published by AgID for a detailed description of the above-mentioned Patterns and of the related underlying processing rules *(please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).*

CHAPTER 5 – APPLICANT ACCESS

The content of this chapter highlights what is reported in Chapter 5 of the " Operative Document: Security Pattern" published by AgID, to which we refer for the detailed explanation of the processing rules, while here we report only the general contents, always following what is reported in Chapter 5 of the above-mentioned document (please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).

5.1 [ID_AUTH_SOAP_01] Direct Trust with X.509 certificate on SOAP

Communication between user and provider that ensures at message level an access of the user, as user organization or organizational unit, or both parties.

Please refer to Chapter 5.1 of the Operative Document related to Security Patterns published by AgID for a detailed description of the above-mentioned patterns and their underlying processing rules *(please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).*

5.2 [ID_AUTH_SOAP_02] Direct Trust with X.509 certificate on SOAP with unique token/message

The following profile extends the ID_AUTH_SOAP_01 profile, and is related to communication between user and provider that ensures at message level:

- Access by the user party, as the user organization or organizational unit, or both;
- defense against attack threats: *Replay Attack*.

Please refer to Chapter 5.2 of the Operative Document related to the Security Patterns published by AgID for a detailed description of the above-mentioned Patterns and of the related underlying processing rules *(please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).*

5.3 [ID_AUTH_REST_01] Direct Trust with X.509 certificate on REST

Communication between user and provider that ensures at message level an access of the user subject, as user organization or organizational unit, or both parties.

Please refer to Chapter 5.3 of the Operative Document related to Security Patterns published by AgID for a detailed description of the above-mentioned Patterns and of the related underlying processing rules *(please refer to the section "Bibliography and Reference Sitography" for the redirect links to the mentioned contents).*

5.4 [ID_AUTH_REST_02] Direct Trust with X.509 certificate on REST with unique token/message

The following profile extends the profile ID_AUTH_REST_01 and is related to the communication between user and provider that ensures at message level:

- access by the user party, as the user organization or organizational unit, or both,
- defense against threats from attacks: Replay Attack when the JWT or the message MUST not be reprocessed.

Please refer to Chapter 5.4 of the Operative Document related to Security Patterns published by AgID for a detailed description of the above-mentioned Patterns and of the related underlying processing rules *(please refer to the section "Bibliography and Reference Sitography" for the redirect links to the mentioned contents).*

CHAPTER 6 – INTEGRITY

The content of this chapter highlights what is reported in Chapter 6 of the " Operative Document: Security Pattern" published by AgID, to which we refer for the detailed explanation of the processing rules, while here we report only the general contents, always following what is reported in Chapter 6 of the above-mentioned document (please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).

6.1 [INTEGRITY_SOAP_01] SOAP message payload integrity

This profile extends ID_AUTH_SOAP_01 or ID_AUTH_SOAP_02, adding the integrity of the message payload to the communication between user and provider at message level.

Please refer to Chapter 6.1 of the Operative Document on Security Patterns published by AgID for a detailed description of the above-mentioned Patterns and their underlying processing rules *(please refer to the section "Reference Bibliography and Sitography" for the redirect links to the above-mentioned contents).*

CHAPTER 7 – SECURITY ISSUES

The content of this chapter highlights what is reported in Chapter 7 of the " Operative Document: Security Pattern" published by AgID, to which we refer for the detailed explanation of the processing rules, while here we report only the general contents, always following what is reported in Chapter 7 of the above-mentioned document (please refer to the section "Reference Bibliography and Sitography" for the redirect links to the mentioned contents).

The algorithms identified for the correct implementation of Security Patterns are listed below:

Transport channel security	In order to ensure authentication, data integrity and confidentiality between the user entity, communications MUST be via HTTPS (HTTP over TLS) communication protocol. Below are listed the minimum cryptographic requirements to establish a secure connection, regarding TLS protocol version, cipher suite: ○ **Protocol Version –** *The minimum version of the TLS protocol MUST be greater than or equal to 1.2 (previous versions MUST not be used),* ○ **Cipher suite –** *Cipher suite to be used MUST support perfect forward secrecy (PFS).*
Digest SOAP	And related SHA/HMAC-SHA (256, 384 e 512)
Signature public key SOAP	And related SHA/HMAC-SHA (256, 384 e 512)
Canonicalization	And related XML/Exclusive XML
Digest and signature public key REST	And related HS/RS/ES (256, 384 e 512)
Digest REST	And related S (256, 384 e 512)

The constant updating of the security elements will be related to the updates carried out by AgID, which will proceed with the issuing of a technical document dedicated to the cipher suite and minimum TLS protocols.

Please refer to Chapter 7 of the Operational Document on Security Patterns edited by AgID for a detailed analysis of the above-mentioned algorithms *(please refer to the section "Bibliography and Reference Sitography" for the redirect links to the mentioned contents).*

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 – Security Patterns

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

Online reference: https://www.agid.gov.it/sites/default/files/repository_files/02_pattern_sicurezza.pdf