TOURISM DIGITAL HUB-TDH022

LINEE GUIDA SULL'INTEROPERABILITÀ TECNICA E LA GESTIONE DELLE API

Documento operativo

Pattern di Sicurezza

Versione 0.1 del 21/12/2021

Versione	Data	Tipologia Modifica
0.1	21/12/2021	Prima Release

Indice Generale

CAPITOLO 1 – INTRODUZIONE

Il presente Documento Operativo descrive i pattern di sicurezza nella comunicazione che gli erogatori *(in tal senso si considerano Soggetti Pubblici quali, a titolo esemplificativo Regioni e Province, oltre che Enti Pubblici o assimilabili e Soggetti Privati, incluse Seconde e Terze Parti che mettono a disposizione del TDH servizi e funzionalità)* attestati all'interno del Tourism Digital Hub devono utilizzare per soddisfare le necessità individuate dai requisiti funzionali e non funzionali delle specifiche interazioni con i relativi fruitori, anch'essi attestati all'interno del Tourism Digital Hub *(in tal senso si considerano invece tutti i soggetti che utilizzano i servizi digitali messi a disposizione dagli erogatori all'interno dell'Ecosistema)*. I pattern di sicurezza descritti in questo Documento Operativo ricalcano quanto indicato nel Documento Operativo "Pattern di Sicurezza[1]" emanato da AgID e collegato al documento "Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni[2]" sempre emanato da AgID; in aggiunta a quanto riportato, si rimanda ai due documenti sopracitati per le indicazioni di dettaglio.

1.1 Pattern di Sicurezza: informazioni preliminari

I Pattern di Sicurezza, dal punto di vista generale, coprono gli aspetti di comunicazione "sicura" tra i domini delle singole parti; tali parti mantengono la loro autonomia negli aspetti organizzativi e di sicurezza interni al proprio dominio; di seguito alcune informazioni di carattere generale in merito:

- Definiscono a livello di specifica tecnologica uno «strumento condiviso» utile a favorire l'interoperabilità tra erogatori e fruitori;
- Forniscono un comune linguaggio per fruitori ed erogatori utile a trattare le necessità e le caratteristiche delle interfacce di servizio;
- Offrono agli sviluppatori le modalità tecniche supportate da standard tecnologici documentati, revisionati e testati per esporre i servizi digitali.

In ultimo, è necessario porre l'accento sulla finalità di tali pattern, ovvero quella di definire le modalità per assicurare che le interazioni tra fruitore ed erogatore (entrambi attestati all'interno del Tourism Digital Hub) siano realizzate nel rispetto delle specifiche esigenze di sicurezza

[1] Riferimento online: https://www.agid.gov.it/sites/default/files/repository_files/02_pattern_sicurezza.pdf
[2] Riferimento online: https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf

determinate dalla natura dell'interscambio di dati, informazioni, contenuti e similari realizzati e dalle prescrizioni normative che li hanno determinati.

L'implementazione dei Pattern di Sicurezza è strettamente correlata a quella dei Pattern di Interazione (cui si applicano) e le relative modalità di implementazione a livello pratico sono scelte dall'erogatore in funzione delle specifiche esigenze applicative di livello tecnico dei fruitori.

Data la costante evoluzione in atto relativamente al contesto tecnologico di riferimento, l'elenco dei Pattern di Sicurezza è in continuo aggiornamento, ed è consultabile presso la Documentazione AgID (si rimanda in tal senso al Capitolo 7 del Documento "Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni" per informazioni di dettaglio in merito).

CAPITOLO 2 – AMBITO DI APPLICAZIONE

Il presente Documento Operativo è redatto quale documento operativo relativo alla Linea di indirizzo sull'interoperabilità tecnica declinata relativamente agli aspetti di sicurezza.

2.1 Soggetti destinatari del documento

Il Documento Operativo è destinato a tutti gli erogatori che mettono a disposizione dei fruitori servizi e funzionalità all'interno del Tourism Digital Hub (TDH) oltre che agli stessi fruitori, nelle more della fruizione dei servizi e delle funzionalità desiderate; queste disposizioni possono dunque essere utilizzare come base per implementazione di nuove funzionalità nel caso in cui debbano essere sviluppate ex-novo ovvero come base per integrazione delle funzionalità esistenti.

Di seguito, *a livello esemplificativo e non esaustivo*, si riporta un elenco dei Soggetti Pubblici e Privati destinatari del Documento Operativo, sia presenti a titolo di erogatori che di fruitori dei servizi e delle funzionalità all'interno del Tourism Digital Hub (TDH).

Soggetti Pubblici

- Pubblica Amministrazione Centrale (es. Ministero del Turismo),
  Pubblica Amministrazione Locale (es. Regioni, Province…),
- Enti Nazionali e Locali (es. ENIT),
- Enti No Profit,
- Imprese pubbliche collegate agli ambiti turistici (es. impianti di risalita…).

Soggetti Privati

- Imprese ricettive, di ristorazione, ecc…,
- Tour Operator/Agenzie di viaggio,
- Sindacati,
- Imprese private collegate agli ambiti turistici (es. impianti di risalita…).

CAPITOLO 3 – RIFERIMENTI E SIGLE

3.1 Note di lettura del documento

Conformemente alle norme ISO/IEC Directives, Part 3 per la stesura dei documenti tecnici il presente Documento Operativo utilizzerà le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «DOVREBBE», «NON DOVREBBE», «PUÒ» e «OPZIONALE», la cui interpretazione è descritta di seguito:

- **DEVE o DEVONO**, indicano un requisito obbligatorio per rispettare la Linea di indirizzo;
- **NON DEVE o NON DEVONO**, indicano un assoluto divieto delle specifiche;
- **DOVREBBE o NON DOVREBBE**, indicano che le implicazioni devono essere comprese e attentamente pesate prima di scegliere approcci alternativi;
- **PUÓ o POSSONO o l'aggettivo OPZIONALE**, indica che il lettore può scegliere di applicare o meno senza alcun tipo di implicazione o restrizione la specifica

3.2 Termini e definizioni[3]

Per una più agevole lettura si riporta un glossario dei termini e delle definizioni contenuti nel presente documento.

[AgID]	Agenzia per l'Italia Digitale
[CAD]	Decreto Legislativo 7 marzo 2005, n. 82 - «Codice dell'Amministrazione Digitale» (noto anche come "CAD"), aggiornato con modifiche dal D.L. 16 luglio 2020 n.76 e convertito in legge con la L. 11 settembre 2020 n.120
[Erogatore]	Uno dei soggetti di cui all'articolo 2, comma 2 del CAD che rende disponibile e-service ad altre organizzazioni, per la fruizione di dati in suo possesso o l'integrazione dei processi da esso realizzati
[Fruitore]	Organizzazione che utilizza gli e-service messi a disposizione da un dei soggetti di cui all'articolo 2, comma 2 del CAD
[REST]	Representational State Transfer

[3] Alcuni termini e definizioni esplicitati all'interno di questo paragrafo sono presenti anche all'interno del documento di "Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni" emanate da AgID

[RPC]	Remote Procedure Call
[SOAP]	Simple Object Access Protocol
[TDH]	Tourism Digital Hub
[TDH022]	TDH022 - Interfaccia di interoperabilità del Tourism Digital Hub
[Trust]	Uno dei mezzi più importanti per gestire le problematiche di sicurezza nello scambio di informazione in rete per consentire l'interoperabilità tra i sistemi. Esso si basa sul reciproco riconoscimento delle entità interagenti e sulla fiducia nei rispettivi comportamenti
[UML]	Linguaggio di modellazione unificato (Unified Modeling Language)

CAPITOLO 4 – SICUREZZA DI CANALE E/O IDENTIFICAZIONE DELLE ORGANIZZAZIONI

Il contenuto di questo capitolo rimarca quanto riportato al Capitolo 4 del "Documento Operativo: Pattern di Sicurezza" edito da AgID, cui si rimanda per l'esplicazione nel dettaglio delle regole di processamento, mentre qui si riportano solo i contenuti di carattere generale, sempre seguendo quanto riportato al Capitolo 4 del documento sopra indicato (si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).

4.1 [ID_AUTH_CHANNEL_01] Direct Trust Transport-Level Security

Relativo alla comunicazione tra fruitore ed erogatore che assicuri, a livello di canale:

- confidenzialità;
- integrità;
- identificazione dell'erogatore, quale organizzazione;
- difesa dalle minacce derivanti dagli attacchi: Replay Attack e Spoofing.

Si rimanda al Capitolo 4.1 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale in merito alla descrizione di dettaglio dei Pattern sopra citati e delle relative regole di processamento sottostanti *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

4.2 [ID_AUTH_CHANNEL_02] Direct Trust mutual Transport-Level Security

Relativo alla comunicazione tra fruitore ed erogatore che assicuri a livello di canale:

- confidenzialità;
- integrità;
- identificazione dell'erogatore e del fruitore, quale organizzazione;
- difesa dalle minacce derivanti dagli attacchi: Replay Attack e Spoofing.

Si rimanda al Capitolo 4.2 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale in merito alla descrizione di dettaglio dei Pattern sopra citati e delle relative regole di processamento sottostanti *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

CAPITOLO 5 – ACCESSO DEL SOGGETTO RICHIEDENTE

Il contenuto di questo capitolo rimarca quanto riportato al Capitolo 5 del "Documento Operativo: Pattern di Sicurezza" edito da AgID, cui si rimanda per l'esplicazione nel dettaglio delle regole di processamento, mentre qui si riportano solo i contenuti di carattere generale, sempre seguendo quanto riportato al Capitolo 5 del documento sopra indicato (si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).

5.1 [ID_AUTH_SOAP_01] Direct Trust con certificato X.509 su SOAP

Comunicazione tra fruitore ed erogatore che assicuri a livello di messaggio un accesso del soggetto fruitore, quale organizzazione o unità organizzativa fruitrice, o entrambe le parti.

Si rimanda al Capitolo 5.1 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale in merito alla descrizione di dettaglio dei Pattern sopra citati e delle relative regole di processamento sottostanti *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

5.2 [ID_AUTH_SOAP_02] Direct Trust con certificato X.509 su SOAP con unicità del token/messaggio

Il seguente profilo estende il profilo ID_AUTH_SOAP_01, ed è relativo alla comunicazione tra fruitore ed erogatore che assicuri a livello di messaggio:

- accesso del soggetto fruitore, quale organizzazione o unità organizzativa fruitore, o entrambe le parti;
- difesa dalle minacce derivanti dagli attacchi: *Replay Attack*.

Si rimanda al Capitolo 5.2 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale in merito alla descrizione di dettaglio dei Pattern sopra citati e delle relative regole di processamento sottostanti *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

5.3 [ID_AUTH_REST_01] Direct Trust con certificato X.509 su REST

Comunicazione tra fruitore ed erogatore che assicuri a livello di messaggio un accesso del soggetto fruitore, quale organizzazione o unità organizzativa fruitore, o entrambe le parti.

Si rimanda al Capitolo 5.3 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale in merito alla descrizione di dettaglio dei Pattern sopra citati e delle relative regole di processamento sottostanti *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

5.4 [ID_AUTH_REST_02] Direct Trust con certificato X.509 su REST con unicità del token/messaggio

Il seguente profilo estende il profilo ID_AUTH_REST_01 ed è relativo alla comunicazione tra fruitore ed erogatore che assicuri a livello di messaggio:

- accesso del soggetto fruitore, quale organizzazione o unità organizzativa fruitore, o entrambe le parti,
- la difesa dalle minacce derivanti dagli attacchi: Replay Attack quando il JWT o il messaggio non DEVONO essere riprocessati.

Si rimanda al Capitolo 5.4 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale in merito alla descrizione di dettaglio dei Pattern sopra citati e delle relative regole di processamento sottostanti *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

CAPITOLO 6 – INTEGRITA'

Il contenuto di questo capitolo rimarca quanto riportato al Capitolo 6 del "Documento Operativo: Pattern di Sicurezza" edito da AgID, cui si rimanda per l'esplicazione nel dettaglio delle regole di processamento, mentre qui si riportano solo i contenuti di carattere generale, sempre seguendo quanto riportato al Capitolo 6 del documento sopra indicato (si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).

6.1 [INTEGRITY_SOAP_01] Integrità del payload del messaggio SOAP

Il presente profilo estende ID_AUTH_SOAP_01 o ID_AUTH_SOAP_02, aggiungendo alla comunicazione tra fruitore ed erogatore a livello di messaggio l'integrità del payload del messaggio.

Si rimanda al Capitolo 6.1 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale in merito alla descrizione di dettaglio dei Pattern sopra citati e delle relative regole di processamento sottostanti *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

CAPITOLO 7 – ASPETTI DI SICUREZZA

Il contenuto di questo capitolo rimarca quanto riportato al Capitolo 7 del "Documento Operativo: Pattern di Sicurezza" edito da AgID, cui si rimanda per l'esplicazione nel dettaglio delle regole di processamento, mentre qui si riportano solo i contenuti di carattere generale, sempre seguendo quanto riportato al Capitolo 7 del documento sopra indicato (si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).

Di seguito sono elencati gli algoritmi individuati per la corretta implementazione dei Pattern di Sicurezza:

Sicurezza del canale di trasporto	Al fine di garantire autenticazione, integrità dei dati e confidenzialità tra ente fruitore, le comunicazioni DEVONO avvenire tramite protocollo di comunicazione HTTPS (HTTP over TLS). Di seguito sono elencate i requisiti crittografici minimi per stabilire una connessione sicura, riguardanti versione del protocollo TLS, cipher suite: ○ **Versione protocollo –** *la versione minima del protocollo TLS DEVE essere maggiore o uguale a 1.2 (Versioni precedenti non DEVONO essere utilizzate),* ○ **Cipher suite –** *Le ciphersuite da utilizzare DEVONO supportare perfect forward secrecy (PFS).*
Digest SOAP	E relativi SHA/HMAC-SHA (256, 384 e 512)
Signature public key SOAP	E relativi SHA/HMAC-SHA (256, 384 e 512)
Canonicalization	E relativi XML/Exclusive XML
Digest and signature public key REST	E relativi HS/RS/ES (256, 384 e 512)
Digest REST	E relativi S (256, 384 e 512)

Il costante aggiornamento degli elementi di sicurezza sarà afferente agli aggiornamenti effettuati a cura di AgID, che procederà con l'emanazione di un documento tecnico dedicato alla cipher suite e protocolli TLS minimi.

Si rimanda al Capitolo 7 del Documento Operativo relativo ai Pattern di Sicurezza edito da AgID per un approfondimento puntuale relativamente agli algoritmi sopra citati *(si rimanda alla sezione "Bibliografia e Sitografia di Riferimento" per i link di redirect ai contenuti citati).*

BIBLIOGRAFIA E SITOGRAFIA DI RIFERIMENTO

Linee Guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni

Autore: AgID – Prima pubblicazione: 27/04/2021

Riferimento online:
https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_interoperabilit_tecnica_pa.pdf

Documento Operativo – Pattern di Sicurezza

Autore: AgID – Prima pubblicazione: 27/04/2021

Riferimento online:
https://www.agid.gov.it/sites/default/files/repository_files/02_pattern_sicurezza.pdf

Immagine di copertina – Credits

Nuvola vettore creata da vectorjuice - it.freepik.com