AGID | Agenzia per l'Italia Digitale

Profili di interoperabilità

Versione 1.0 del 27/04/2021

AGID | via Liszt, 21 – 00144 Roma | protocollo@pec.agid.gov.it | www.agid.gov.it | tel. 06 85264.1

Versione	Data	Tipologia modifica
1	27/04/2021	Prima emissione

Sommario

Introduzione

I profili di interoperabilità individuano combinazioni dei pattern di interazione, indicati nel Documento Operativo - Pattern di interazione, e pattern di sicurezza, indicati Documento Operativo - Pattern di sicurezza, che risolvono una esigenza specifica della comunicazione tra fruitore ed erogatore.

I profili di interoperabilità sono scelti dall'erogatore in funzione alle specifiche esigenze applicative ed in relazione alla natura dei fruitori.

Data la variabilità nel tempo delle esigenze delle amministrazioni e delle tecnologie abilitanti, nonché considerata la natura incrementale del ModI, l'elenco dei profili non è da intendersi esaustivo. Nel caso in cui un'amministrazione abbia esigenze non ricoperte nei seguenti profili DEVE informare AgID, nei modi indicati nel capitolo 7 «Pattern e profili di interoperabilità» delle Linee di indirizzo sull'interoperabilità tecnica delle Pubbliche Amministrazioni. Le tecnologie e standard per assicurare la sicurezza dell'interoperabilità tramite API utilizzabili nel ModI, tra cui OAuth 2.0, sono individuate nelle Linee Guida sulla sicurezza, emanate dall'Agenzia per l'Italia Digitale ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale).

Capitolo 1

Ambito di applicazione

Il presente Documento operativo è redatto quale documento operativo relativo alla Linee Guida sull'interoperabilità tecnica..

1.1 Soggetti destinatari

Il Documento Operativo è destinato ai soggetti di cui all'articolo 2, comma 2 del CAD, così come indicato dall'articolo 75 dello stesso. I destinatari la attuano nella realizzazione dei propri sistemi informatici che fruiscono o erogano dati e/o servizi digitali ad altri soggetti.

Il Documento Operativo è rivolto ai soggetti privati che devono interoperare con la Pubblica Amministrazione per erogare o fruire di dati e servizi tramite sistemi informatici.

Capitolo 2

Riferimenti e sigle

2.1 Note di lettura del documento

Conformemente alle norme ISO/IEC Directives, Part 3 per la stesura dei documenti tecnici la presente linea guida utilizzerà le parole chiave «DEVE», «DEVONO», «NON DEVE», «NON DEVONO», «E" RICHIESTO», «DOVREBBE», «NON DOVREBBE», «RACCOMANDATO», «NON RACCOMANDATO» «PUO"» e «OPZIONALE», la cui interpretazione è descritta di seguito.

- **DEVE** o **DEVONO**, indicano un requisito obbligatorio per rispettare la linea guida;
- **NON DEVE** o **NON DEVONO**, indicano un assoluto divieto delle specifiche;
- **DOVREBBE** o **RACCOMANDATO** o **NON DOVREBBE** o **NON RACCOMANDATO**, 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 la specifica.

2.2 Standard di riferimento

Sono riportati di seguito gli standard tecnici indispensabili per l'applicazione del presente documento.

[X.509] Standard dell'Unione Internazionale delle telecomunicazioni (ITU-T), che definisce definire il formato dei certificati a chiave pubblica e delle autorità di certificazione

2.3 Termini e definizioni

Di seguito si riportano gli ACRONIMI che verranno utilizzati nella presente Linee Guida:

[AgID] Agenzia per l'Italia Digitale

[CAD] Codice Amministrazione Digitale, D.lgs. 7 marzo 2005, n. 82

[PA]	Pubblica Amministrazione
[UML]	Linguaggio di modellazione unificato (Unified Modeling Language)
[RPC]	Remote procedure call
[SOAP]	Simple Object Access Protocol
[REST]	Representational State Transfer

Capitolo 3

Profili di interoperabilità

Di seguito le indicazioni per le tecnologie accolte dal ModI.

L'AgID assicura l'aggiornamento degli stessi per soddisfare le esigenze espresse dalle PA.

3.1 [PROFILE_CONF_ID_AUTH_01] Profilo per confidenzialità ed autenticazione del fruitore

Dare seguito ad uno scambio tra fruitore ed erogatore che garantisca:

- la confidenzialità a livello di canale
- l'autenticazione del fruitore

Il fruitore potrebbe non coincidere con l'unità organizzativa fruitore, ma comunque appartenere alla stessa.

Questo profilo è indipendente dal pattern di interazione implementato ed utilizza i seguenti pattern di sicurezza:

- ID_AUTH_CHANNEL_01
- ID_AUTH_SOAP_01 o ID_AUTH_REST_01

Si assume l'esistenza di un trust tra fruitore ed erogatore che stabilisce:

- riconoscimento da parte dell'erogatore dei certificati X.509, o la CA emittente, relative al fruitore
- riconoscimento da parte del fruitore del certificato X.509, o la CA emittente, relative al soggetto erogatore

Il meccanismo con cui è stabilito il trust non condiziona quanto descritto di seguito.

3.1.1 Flusso delle interazioni

A: Richiesta

Il messaggio di richiesta viene predisposto utilizzando il pattern [ID_AUTH_SOAP_01] nel caso di utilizzo di SOAP o [ID_AUTH_REST_01] nel caso di utilizzo di REST, per garantire:

- l'identità del fruitore.

Il fruitore invia il messaggio di richiesta all'interfaccia di servizio dell'erogatore.

Il messaggio viene trasmesso su un canale sicuro utilizzando il profilo ID_AUTH_CHANNEL_01 per garantire:

- la confidenzialità a livello di canale.

B: Risposta

L'erogatore da seguito a quanto previsto nel pattern ID_AUTH_SOAP_01 nel caso di utilizzo di SOAP o ID_AUTH_REST_01 nel caso di utilizzo di REST.

3.2 [PROFILE_NON_REPUDIATION_01] Profilo per la non ripudiabilità della trasmissione

Dare seguito ad uno scambio tra fruitore ed erogatore che garantisca la non ripudiabilità assicurando a livello di messaggio:

- integrità del messaggio
- autenticazione del fruitore, quale organizzazione o unità organizzativa fruitore quale mittente del contenuto
- conferma da parte dell'erogatore della ricezione del contenuto
- opponibilità ai terzi
- robustezza della trasmissione

Il presente profilo utilizza come modello di comunicazione il Pattern di interazione BLOCK_SOAP nel caso di utilizzo di SOAP o BLOCK_REST nel caso di utilizzo di REST. Questo profilo utilizza i seguenti pattern di sicurezza:

- ID_AUTH_CHANNEL_01 o in alternativa ID_AUTH_CHANNEL_02
- per SOAP: ID_AUTH_SOAP_02 e INTEGRITY_SOAP_01
- per REST: ID_AUTH_REST_02 e INTEGRITY_REST_01

Si assume l'esistenza di un trust tra fruitore ed erogatore che stabilisce:

- reciproco riconoscimento da parte dell'erogatore e del fruitore dei certificati X.509, o le CA emittenti.
- Il meccanismo con cui è stabilito il trust non condiziona quanto descritto nella sezione. Fruitore ed erogatore devono concordare:
    - un identificativo univoco del messaggio, necessario a garantire il riscontro di ritrasmissioni (vedi ID_AUTH_SOAP_02 e ID_AUTH_REST_02), e le relative modalità di scambio;
    - l'arco temporale di persistenza dei messaggi, che dipende dalle caratteristiche del contenuto dei dati scambiati e dal rispetto delle norme di legge.
    - il tempo di validità della transazione che intercorre tra:
        - l'istante di inoltro del fruitore
        - l'istante di ricezione dell'erogatore;
    - il tempo massimo di attesa del fruitore del messaggio di risposta per ritenere la comunicazione non avvenuta;
    - il numero massimo di tentativi di rinvio da parte del fruitore accettati dall'erogatore;
    - eventuale utilizzo di canali alternativi per superare o evidenziare problemi di comunicazione riscontrati.
- Attraverso le tecnologie di criptazione sono garantite le seguenti proprietà:
    - integrità e non ripudio del messaggio inviato dal fruitore
    - integrità e non ripudio del messaggio di conferma da parte dell'erogatore
    - autenticazione del fruitore
    - autenticazione dell'erogatore
    - validazione temporale che certifichi l'istante in cui il messaggio è stato trasmesso
    - validazione temporale che certifichi l'istante in cui il messaggio è stato ricevuto.

3.2.1 Flusso delle interazioni

A: Verifica numero tentativi di inoltro

Il fruitore realizza una delle seguenti azioni:

A.1 [Primo Invio]

Il fruitore inizializza il numero di tentativi di inoltro ad 1 e prosegue a quanto indicato al passo B.

A.2 [Invio Successivo con numero di tentativi inferiore al massimo pattuito]

Il fruitore incrementa il numero di tentativi di inoltro e da seguito a quanto indicato al passo B.

A.3 [Superamento numero di tentativi massimi pattuiti]

Il fruitore utilizza i canali alternativi per superare o evidenziare problemi di comunicazione riscontrati non proseguendo con i passi successivi.

B: Richiesta

Il messaggio di richiesta viene costruito aggiungendo un identificativo univoco del messaggio (vedi [ID_AUTH_SOAP_02] o [ID_AUTH_REST_02]), l'istante di trasmissione

- SOAP: <wsu:Timestamp> della ws-security
- REST: claim iat contenuta nel payload del token JWT

Tutti gli elementi utili al non ripudio, inclusi quelli descritti in ID_AUTH_SOAP_02 o ID_AUTH_REST_02, vengono firmati utilizzando il profilo desiderato INTEGRITY_SOAP_01 o INTEGRITY_REST_01 per garantire:

- l'integrità del contenuto
- l'identità del mittente
- il momento di invio.

Il fruitore invia il messaggio di richiesta all'interfaccia di servizio dell'erogatore. Il messaggio viene trasmesso su un canale sicuro per garantire:

- la confidenzialità a livello di canale utilizzando i pattern ID_AUTH_CHANNEL_01 o in alternativa ID_AUTH_CHANNEL_02.

C. Persistenza erogatore

Per garantire la non ripudiabilità del messaggio ricevuto dal fruitore, così come previsto dai profili utilizzati:

- L'erogatore provvede all'autenticazione del fruitore;

- L'erogatore verifica l'integrità del messaggio firmato. Inoltre la presenza dell'istante di trasmissione nel messaggio ne garantisce validità a lungo termine.

Per assicurare l'opponibilità a terzi:

- L'erogatore rende persistente il messaggio firmato tracciando l'istante di ricezione.

La persistenza del messaggio:

- DEVE garantire la capacità di ricercare ed esportare le informazioni memorizzate;
- DEVE essere garantita per un periodo di tempo che dipende dagli accordi tra le parti.

L'erogatore realizza una delle seguenti azioni:

C.1 [Prima Ricezione]

L'erogatore inizializza il numero di tentativi di richieste ricevute ad 1 e prosegue al passo D.

C.2 [Duplicato con numero di tentativi inferiore al massimo pattuito]

L'erogatore rileva la presenza di un identificativo univoco del messaggio già ricevuto, a causa di una mancata ricezione del messaggio di conferma da parte del fruitore. Incrementa il numero di tentativi di richieste ricevute e prosegue al passo D.

C.3 [Superamento numero massimo di tentativi pattuiti]

L'erogatore rileva la presenza di un identificativo univoco del messaggio già ricevuto, a causa di una mancata ricezione del messaggio di conferma da parte del fruitore.

L'erogatore rileva di aver raggiunto il numero massimo di tentativi di richieste ricevute. L'erogatore utilizza i canali alternativi per superare o evidenziare problemi di comunicazione riscontrati non proseguendo con i passi successivi.

D: Risposta

L'erogatore costruisce un messaggio di conferma includendo un identificativo che permetta di associare univocamente al messaggio di richiesta (ad esempio il digest presente nel messaggio di richiesta) e l'istante di trasmissione.

Inoltre al messaggio di conferma viene aggiunto l'istante di trasmissione:

- SOAP: <wsu:Timestamp> della ws-security
- REST: claim iat contenuta nel payload del token JWT

Tutti gli elementi utili al non ripudio, inclusi quelli descritti in ID_AUTH_SOAP_02 o ID_AUTH_REST_02, vengono firmati utilizzando il profilo desiderato INTEGRITY_SOAP_01 o INTEGRITY_REST_01 per garantire:

- l'integrità del contenuto
- l'identità del mittente
- il momento di invio

E: Persistenza Richiedente

Per garantire la non ripudiabilità del messaggio inviato all'erogatore:

- Il fruitore provvede all'autenticazione dell'erogatore rispetto al messaggio di risposta.
- Il fruitore verifica l'integrità del messaggio di risposta firmato in cui la presenza del timestamp sul protocollo di messaggio ne garantisce validazione a lungo termine e il tempo di ricezione.

Per assicurare l'opponibilità a terzi:

- Il fruitore rende persistente il messaggio di risposta firmato.

La persistenza del messaggio:

- DEVE garantire la capacità di ricercare ed esportare le informazioni memorizzate;
- DEVE essere garantita per un periodo di tempo che dipende dagli accordi tra le parti.

Note:

Nel caso in cui il fruitore non riceve il messaggio di risposta entro i termini concordati tra le parti, si ritiene la comunicazione non conclusa, in quanto può presentarsi uno dei seguenti casi:

- il messaggio di richiesta non ha raggiunto l'erogatore
- il messaggio di richiesta ha raggiunto l'erogatore ma il fruitore non ha ricevuto il messaggio di risposta.

In queste situazioni il fruitore riesegue il passo A.

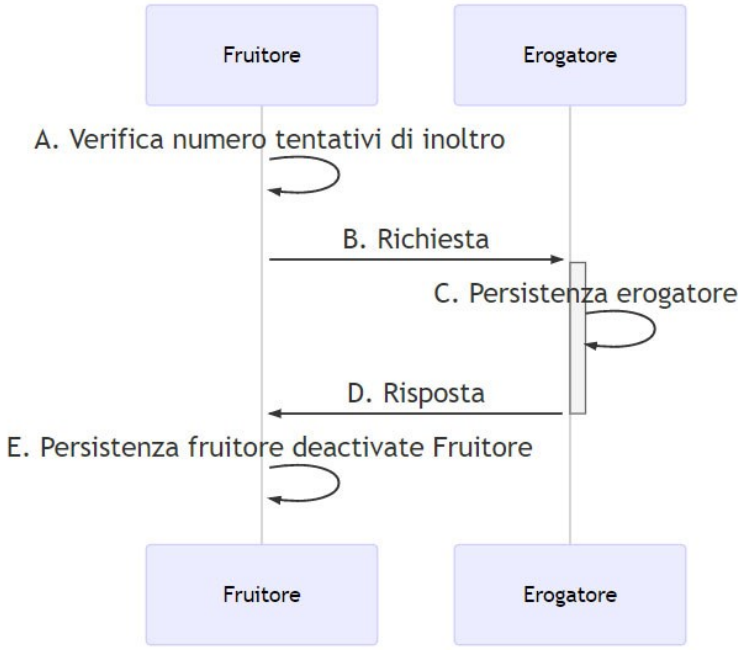

Figura 1 - Non ripudiabilità della trasmissione