Linee guida pubblicazione API in E015 Digital Ecosystem

version 0.0.1

AUTORE

11 January 2018

Indice

Linee guida per la pubblicazione di API in E015 Digital Ecosystem

Processo di pubblicazione delle API in E015 Digital Ecosystem

Il presente documento indica le modalità operative e le Linee Guida tecnologiche che è necessario seguire al fine di poter pubblicare una API all'interno di E015 Digital Ecosystem. La pubblicazione delle API all'interno di E015 Digital Ecosystem avviene in modo controllato, in accordo a un processo di pubblicazione ben preciso che prevede l'interazione tra l'API Provider e l'Ecosistema stesso. Tale processo di pubblicazione è raffigurato in Figura 1.1.

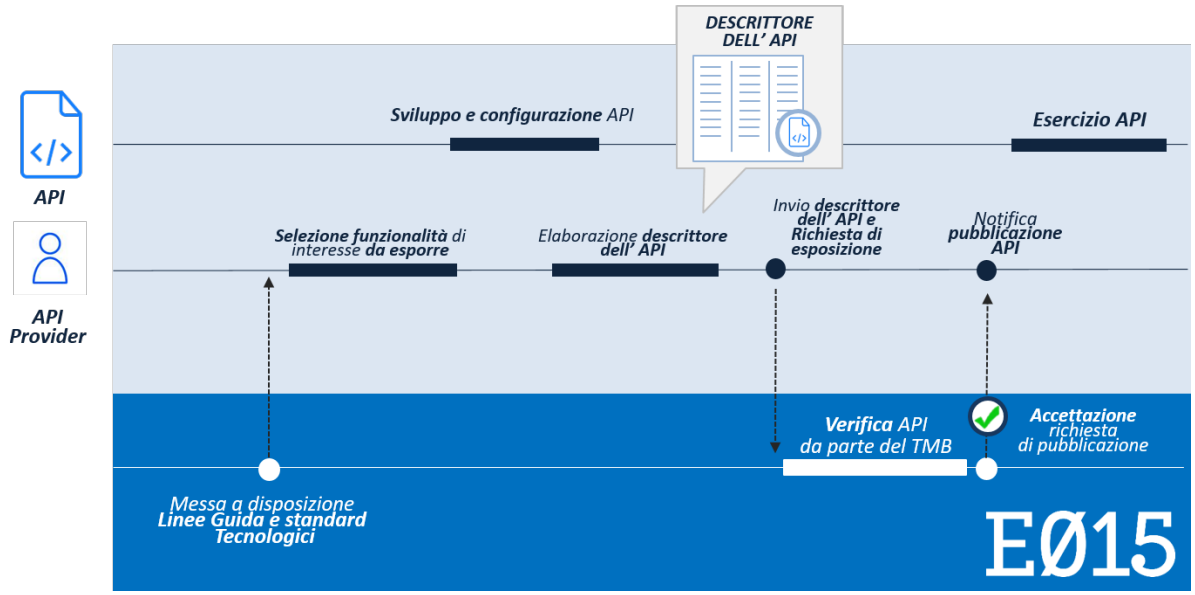

Figura 1.1: Processo di pubblicazione delle API in E015 Digital Ecosystem (da sinistra a destra il flusso delle attività che ogni soggetto svolge e la corrispondente sincronizzazione)

Viene riportata nel seguito una descrizione di tutti i passi che caratterizzano il processo di pubblicazione di API all'interno dell'Ecosistema.

Si precisa che le interazioni tra l'API Provider e l'Ecosistema sono supportate da un ambiente di relazione disponibile online attraverso il quale gestire le richieste di pubblicazione delle API ed i necessari scambi informativi (incluse eventuali notifiche).

Descrizione delle fasi del processo di pubblicazione di una API

Fase del processo	Descrizione
Selezione funzionalità di interesse da esporre	L'API Provider identifica le funzionalità di interesse che ritiene opportuno esporre sotto forma di API all'interno di E015 Digital Ecosystem. Tale valutazione di opportunità viene eseguita dall'API Provider in accordo alle proprie strategie aziendali o al proprio ruolo istituzionale. Le funzionalità che l'API Provider può decidere di mettere a disposizione sotto forma di API all'interno dell'Ecosistema riguardano in generale informazioni o funzionalità specifiche dell'API Provider stesso, direttamente o indirettamente correlate al proprio settore di attività.
Sviluppo e configurazione API	Le API che possono essere pubblicate all'interno di E015 Digital Ecosystem devono essere realizzate secondo gli standard tecnologici e le Linee Guida riportate nel presente documento. Non sono ammesse eccezioni.
Elaborazione descrittore dell'API	Questa attività ha come scopo principale la compilazione del documento che descrive ogni API da pubblicare. Tale documento – che prende il nome di "Descrittore dell'API" – è di fondamentale importanza per l'Ecosistema e riassume le principali informazioni dell'API. Esso consente agli App Provider di valutare l'opportunità di utilizzare l'API. Tale documento presenta in allegato il manuale tecnico con le specifiche di utilizzo dell'API e le policy di utilizzo dell'API (definite dall'API Provider).
Invio descrittore dell'API e richiesta di esposizione	L'API Provider invia all'Ecosistema il "Descrittore dell'API" compilato in ogni sua parte, unitamente ad una richiesta di pubblicazione dell'API stessa; in questo modo l'API Provider si rende disponibile affinché il Technical Management Board possa effettuare le verifiche necessarie per approvare o meno la richiesta di pubblicazione dell'API.
Verifica API	Il Technical Management Board prende in carico la richiesta di pubblicazione trasmessa dall'API Provider e procede con le attività di verifica necessarie. I dettagli sulla procedura di verifica dell'API da parte del Technical Management Board sono forniti nel Capitolo 3 del presente documento.

Accettazione richiesta di pubblicazione	Nel caso in cui tutte le verifiche effettuate siano andate a buon fine, il Technical Management Board accetta la richiesta di pubblicazione dell’API inviata da parte dell’API Provider. Il Technical Management Board registra e archivia il descrittore dell’API e inserisce parte delle informazioni in esso contenute all’interno del Catalogo delle API ufficialmente pubblicati all’interno dell’ambiente di relazione dell’ecosistema. Qualora la richiesta di pubblicazione non possa essere accettata (ad esempio, per motivi di non conformità dell’API con le Linee Guida tecnologiche dell’Ecosistema), il TMB interagirà con l’API Provider al fine di indirizzare le problematiche riscontrate e favorire in questo modo l’accettazione della richiesta di pubblicazione.
Notifica pubblicazione API	E015 Digital Ecosystem inoltra all’API Provider la notifica di accettazione della richiesta di pubblicazione. L’API Provider è invitato a segnalare al Technical Management Board le applicazioni proprie che utilizzano la medesima API pubblicata all’interno dell’Ecosistema. Tali applicazioni possono mostrare il logo E015 indicando la frase standard (o equivalente): «Parte delle informazioni e delle funzionalità utilizzate sono richiedibili nella forma di API all’interno dell’Ecosistema Digitale E015”.
Esercizio API	L’API Provider eroga l’API in accordo alle Linee Guida dell’Ecosistema e secondo gli impegni assunti verso l’Ecosistema tramite il “Descrittore dell’API”. Il Technical Management Board di E015 potrà svolgere attività di comunicazione in merito all’API appena pubblicata verso gli aderenti all’Ecosistema o altri soggetti interessati.

Si precisa che durante tutte le fasi sopra riportate il Technical Management Board è a disposizione degli API Provider e svolge un ruolo di supporto e di facilitazione al fine di consentire ai soggetti aderenti di poter portare a termine con successo le procedure di pubblicazione delle proprie API. Si precisa inoltre che tutte le indicazioni e le Linee Guida specifiche per poter portare a termine con successo la procedura di pubblicazione delle API sono rese disponibili agli API Provider all’interno dell’ambiente di relazione dell’Ecosistema.

Descrittore dell’API

L’elemento cardine per la pubblicazione delle API all’interno di E015 Digital Ecosystem è rappresentato dal “Descrittore dell’API”. Il “Descrittore dell’API” indirizza nel suo complesso tematiche di tipo tecnologico – per consentire l’integrazione delle API all’interno delle applicazioni –e fornisce numerose informazioni sull’API, tenendo in considerazione aspetti di tipo organizzativo e di policy che regolamentano l’utilizzo dell’API stessa. In Figura 2.1 sono

riportate tutte le caratteristiche necessarie alla documentazione delle API condivise all’interno dell’Ecosistema, da dettagliare nel documento specifico.

Figura 2.1: Dimensioni di interesse per la descrizione delle API di E015 Digital Ecosystem

È necessario che ognuna di queste dimensioni sia adeguatamente documentata affinché una API possa essere pubblicata all’interno dell’Ecosistema. Di seguito un breve riassunto delle dimensioni di interesse indirizzate dal “Descrittore dell’API”:

- Aspetti di interoperabilità: rientrano in questa categoria tutti gli aspetti di tipo tecnico necessari per poter invocare le API pubblicate all’interno dell’Ecosistema ed integrarle all’interno delle Applicazioni (per esempio, la documentazione dell’interfaccia dell’API);
- Accesso sicuro alle API: rientrano in questa categoria tutti gli aspetti tecnologici ed organizzativi necessari per la gestione degli aspetti di sicurezza legati all’erogazione delle API (ad esempio, per la restrizione dell’accesso alle API ai soli soggetti autorizzati da parte dell’API Provider, per mezzo di uno specifico meccanismo in seguito denominato “meccanismo di attestazione”);
- Glossari delle API: aspetti di documentazione legati al modello dei dati gestiti dalla API (entità, concetti e loro rappresentazione);
- Aspetti di monitoraggio delle API: rientrano in questa categoria tutti gli aspetti necessari affinché E015 Digital Ecosystem sia in grado di monitorare costantemente la disponibilità delle API messe a disposizione da parte degli API Provider;
- Aspetti correlati all’erogazione delle API: rientrano in questa categoria gli aspetti riguardanti eventuali “Logiche di remunerazione” correlate all’utilizzo delle API e gli aspetti di “Qualità” di erogazione delle API;
- Aspetti legati all’azienda: rientrano in questa categoria gli aspetti di tipo organizzativo e di comunicazione, correlati all’erogazione delle API (es: referente dell’API verso E015 Digital Ecosystem);
- Policies delle API: sezione del descrittore riportante i termini e le condizioni di utilizzo con cui sono esposte le API sull’Ecosistema e che ciascun soggetto utilizzatore dell’API si deve impegnare a rispettare nei confronti dell’API Provider.

Nei prossimi paragrafi vengono forniti tutti i dettagli e le indicazioni operative per indirizzare ciascuna di queste dimensioni.

Aspetti di interoperabilità

Gli aspetti di interoperabilità all’interno del descrittore dell’ API

Si riportano nella tabella seguente i campi del descrittore dell’API che indirizzano direttamente gli aspetti legati all’interoperabilità delle API.

Descrittore dell’API

Campi del descrittore relativi agli aspetti di interoperabilità

Fase del processo	Descrizione
Tecnologia	Tecnologia di riferimento con la quale l’API è stata implementata.
Interfaccia dell’API	Riferimento a uno o più file allegati al descrittore che documentano l’interfaccia dell’API in modo completo per un utilizzatore. Per favorire l’interoperabilità all’interno dell’Ecosistema, il descrittore deve sempre contenere, in uno degli allegati, almeno un esempio di tracciato dati per ogni entità restituita. Tali documenti devono essere condivisi in formato editabile in modo che il Technical Management Board possa rimuovere gli endpoint dalla documentazione disponibile all’interno dell’ambiente di relazione. Tali endpoint non devono contenere indirizzi IP espliciti (es. 10.10.10.10) ma sempre nomi simbolici.
Modello dei dati	Riferimento a uno o più file allegati al descrittore che documentano la struttura delle richieste e delle risposte in modo completo per un utilizzatore.
Pattern di interazione interazione	Paradigma di interazione con l’API. I valori ammissibili per questo attributo del descrittore sono: 1. Request-response; 2. Publish & subscribe;

Sono riportate nel seguito gli standard tecnologici e le relative linee guida per la gestione degli aspetti di interoperabilità delle API di E015 Digital Ecosystem. In particolare, le API di E015 Digital Ecosystem possono essere realizzate secondo uno dei due seguenti standard tecnologici:

- SOAP (Simple Object Access Protocol);
- REST (REpresentational State Transfer).

Stardard tecnologici e Linee Guida per l’interoperabilità

Tecnologie per le API SOAP

I Web Service SOAP rappresentano un meccanismo consolidato, condiviso e diffuso a supporto delle interazioni applicative ‘machine-to-machine’. La Web Services Interoperability Organization (WS-I, http://www.oasis-ws-i.org/), ha assunto il compito di definire profili di interoperabilità standard tra Web Service SOAP a diversi livelli. Ciascun profilo raccomanda un insieme “minimo” coerente di specifiche standard non proprietarie per promuovere e realizzare l’interoperabilità tra Web Service SOAP. Tra i profili WS-I, il WS-I Basic Profile (BP) si occupa in particolare di normare le dimensioni tecnologiche basilari per l’interoperabilità tra Web Services (la specifica dell’interfaccia, la rappresentazione del modello dei dati, i meccanismi di trasporto e scambio messaggi ecc.). Esistono attualmente diverse versioni del

WS-I Basic Profile (v1.0 errata: 25 ottobre 2005, v1.1 final: 10 aprile 2006, v1.2 e v2.0 final: 9 novembre 2010), le più recenti delle quali sono riassunte nella tabella che segue. Per ciascuna versione del BP la tabella riassume le tecnologie citate, raggruppate per categoria, evidenziando le principali differenze e le novità rispetto alla versione precedente del profilo.

Figura 2.2: Versioni del WS-I Basic Profile a confronto

Il punto di riferimento iniziale a supporto dell'interoperabilità dei Web Services SOAP in E015 Digital Ecosystem è il WS-I Basic Profile versione 1.1.

Inoltre, a corredo o a complemento delle diverse versioni del BP, la OASIS WS-I organization ha definito i seguenti profili:

- Simple SOAP Binding Profile (v1.0 final: 24 agosto 2004): indica requisiti specifici sulla serializzazione delle buste SOAP e la relativa rappresentazione nei messaggi di richiesta e risposta.
- Attachments Profile (v1.0 final: 20 aprile 2006): complementare al BP 1.1 relativamente all'uso di SOAP with Attachments.
- Basic Security Profile (v1.0 final errata: 5 luglio 2010, v1.1 final: 24 gennaio 2010): Fornisce requisiti specifici per rappresentare e veicolare le informazioni di sicurezza legate a un Web API. Le considerazioni relative alla sicurezza dei API SOAP sono riportate nella Sezione 2.2.4.1.

Considerazioni sul modello dei dati

La selezione congiunta di un sottoinsieme di tecnologie standard è un elemento abilitante per l'interoperabilità applicativa; tuttavia è necessario indirizzare altri aspetti legati all'interoperabilità e relativi alle modalità di utilizzo degli standard tecnologici selezionati. Da questo punto di vista, il modello dei dati su cui si basano le interfacce delle API riveste un ruolo di particolare importanza. In generale, le specifiche dei Web API non entrano nel merito del modello dei dati di una API. Per garantire l'interoperabilità e la qualità delle API esposte in

E015 Digital Ecosystem, in aggiunta alle specifiche tecniche, occorre introdurre opportune linee guida relative al modello dei dati e in generale all’interfaccia di una API.

Uso di XLM Schema

- È opportuno fare riferimento a tipi standard della specifica XML Schema anziché creare tipi “custom” (esempi: ‘xs:date’, ‘xs:duration’, ‘xs:gYear’);
- Si sconsiglia di utilizzare tipi generici (es. ‘xs:string’) per rappresentare dati strutturati;
- In caso di campi alfanumerici aventi una formattazione specifica, è opportuno restringere l’uso del tipo ‘xs:string’ utilizzando opportuni pattern (esempi: ‘CAP’, ‘codice fiscale’, ‘codice Istat comune’);
- Valutare sempre l’uso di tipi già definiti nei Glossari condivisi dell’Ecosistema (esempi: ‘visitatore’, ‘point of interest’, ‘evento’).

WSDL(http://www.w3.org/TR/wsdl) e parametri di input e output

- Si sconsiglia di utilizzare tipi “opachi” (per esempio in formato ‘base64binary’) nei parametri di input e output di una API: l’uso di tipi non opachi abilita controlli strutturali (validazione rispetto allo schema XML) che possono essere effettuati già a livello di interfaccia anziché essere rimandati a livello applicativo affidandoli alla logica interna di funzionamento del singolo API.
- Adottare sempre, quando possibile, il Document/Literal Style.

Tecnologie per le API REST

Le API REST rappresentano una modalità alternativa per la pubblicazione e fruizione di API su protocollo HTTP rispetto a API di tipo SOAP. REST non impone particolari vincoli sulle tecnologie da adottare, per esempio relativamente alla descrizione dell’interfaccia o al modello dei dati. Tuttavia esistono alcune specifiche che possono essere utilizzate in ambito REST per coprire determinate dimensioni di interoperabilità (es. OpenAPI/Swagger per la descrizione dell’interfaccia di un API).

Le API REST pubblicate in E015 Digital Ecosystem devono essere accompagnate da una adeguata documentazione, in particolare per quanto riguarda:

- Il modello e il formato dei dati;
- Le operazioni fornite dalla API.

Il presente requisito può essere soddisfatto allegando una descrizione dell’API formulata mediante uno dei linguaggi di descrizione di API REST quali, ad esempio, OpenAPI 3.0, OpenAPI 2.0 (anche noto come Swagger 2.0). Il linguaggio di descrizione OpenAPI è attualmente supportato dal consorzio Open API Initative (https://www.openapis.org/). In alternativa, per il modello dei dati delle API REST si richiede di utilizzare in particolare:

- XML Schema (http://www.w3.org/XML/Schema) per i dati in formato XML;
- JSON Schema (http://json-schema.org/) per i dati in formato JSON.

Per la pubblicazione e il discovery di API REST si può fare riferimento agli standard Atom (http://www.ietf.org/rfc/rfc4287.txt). Per realizzare la sicurezza di canale è opportuno utilizzare sempre il protocollo HTTPS. Per ulteriori considerazioni relative alla sicurezza dei API REST si veda la Sezione 2.2.4.2.

Tecnologie per le API Publish/Subscribe

E015 Digital Ecosystem intende supportare scenari in cui da una parte vi sono soggetti, per esempio le API, che pubblicano notifiche (notify) e dall’altra vi sono altri soggetti, per

esempio le applicazioni, che sono interessati a ricevere notifiche per erogare le proprie funzionalità (subscribe).

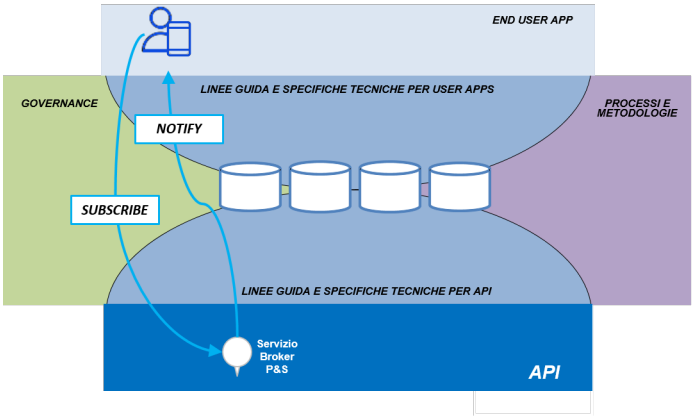

Figura 2.3: Approccio al publish/subscribe nell’Ecosistema

Nell’ambito dell’Ecosistema è possibile adottare i seguenti due approcci (non mutuamente esclusivi) al Publish/Subscribe:

- Notification Dispatcher pubblicato dal singolo API Provider: in questo caso è il singolo provider dell’API a implementare internamente la logica di subscribe e notify necessaria a supportare il funzionamento della propria API (es. propagazione di informazioni ai soggetti interessati);
- Broker Publish/Subscribe esposto da un API Provider: in questo caso l’API di sottoscrizione e notifica è fornita come API trasversale erogata da un provider di E015 Digital Ecosystem e messa a disposizione di altri soggetti. Per esempio, può trattarsi di API di notifica dedicate destinate a domini verticali o specifiche categorie di eventi.

La tecnologia di riferimento è WS-Notification (http://www.oasis-open.org/committees/wsn/), attuale specifica di riferimento in ambito Web Service SOAP. Nel caso in cui si intendesse pubblicare all’interno dell’Ecosistema una API di tipo Publish/Subscribe è necessario assegnare all’attributo “Pattern di interazione” del descrittore dell’API il valore Publish&Subscribe. Qualora invece si intendesse pubblicare una API sincrona di tipo request-response è necessario assegnare all’attributo “Pattern di interazione” del descrittore del API il valore Request-Response.

Accesso sicuro alle API

Gli aspetti di sicurezza all’interno del descrittore dell’API

Si riportano nella tabella seguente i campi del descrittore che indirizzano direttamente gli aspetti legati all’accesso sicuro alle API.

Campi del descrittore relativi all’accesso sicuro alle API

Campo	Descrizione

Descrittore dell’API

Livello di accesso	Indicazione del livello di accesso previsto per l’API. I valori ammissibili sono: 1. Community: per API accessibili da parte di qualsiasi applicazione dell’Ecosistema; 2. Restricted: per API con accesso limitato alle sole applicazioni dell’Ecosistema esplicitamente autorizzate.
Attestazione Client	Riferimento al certificato d’accesso utilizzato
Aspetti di sicurezza specifici	Riferimento a uno o più file allegati al descrittore che documentano eventuali aspetti di sicurezza specifici che è necessario conoscere per utilizzare correttamente l’API.

L’approccio dell’Ecosistema per l’accesso sicuro alle API da parte delle Applicazioni

Nell’ambito di E015 Digital Ecosystem l’API Provider, per ciascuna delle API erogate, deve esplicitare all’interno del descrittore se intende consentire l’accesso a tutte le applicazioni dell’Ecosistema (senza la necessità di una autorizzazione esplicita) oppure se intende restringere l’accesso alle sole applicazioni autorizzate. In particolare all’interno del descrittore, relativamente alla sezione “Accesso all’API”, sarà possibile selezionare una delle seguenti opzioni per l’attributo “Livello di accesso”:

1. Community: L’API è accessibile da parte di tutte le applicazioni dell’Ecosistema senza la necessità di una autorizzazione esplicita da parte dell’API Provider. L’Ecosistema invia all’API Provider una notifica ogni qualvolta una API di tipo community viene richiesta da parte di un App Provider. In questo modo E015 Digital Ecosystem consente all’API Provider di essere a conoscenza di quali siano gli utilizzatori della propria API.
2. Restricted: L’accesso è consentito alle sole applicazioni esplicitamente autorizzate da parte dell’ API Provider. In questo caso, l’Ecosistema inoltra agli API Provider le eventuali richieste di utilizzo ricevute da parte dei soggetti interessati e tiene traccia della risposta specificata da parte degli API Provider (di tipo “allow” / “deny”). In questo modo, E015 Digital Ecosystem è in grado di stabilire, ad un dato momento, quali applicazioni sono state esplicitamente autorizzate all’accesso. L’API Provider ha la possibilità in ogni momento di revocare l’accesso all’API da parte di una applicazione, ad esempio in seguito alla rilevazione di una violazione dei relativi termini di utilizzo [1].

Il meccanismo attraverso il quale E015 Digital Ecosystem consente agli API Provider di gestire la restrizione dell’accesso alle proprie API a tutte le applicazioni dell’Ecosistema (nel caso di API di tipo Community) o alle sole applicazioni dell’Ecosistema esplicitamente autorizzate (nel caso di API Restricted) prende il nome di “Meccanismo di attestazione”.

Grazie al meccanismo di attestazione le API hanno la possibilità di determinare a quali applicazioni dell’Ecosistema appartengono le invocazioni ricevute.

Da un punto di vista operativo, la gestione dell’accesso sicuro alle API impatta su due fasi specifiche del processo di pubblicazione di una API:

1. Descrizione dell’API: In fase di compilazione del descrittore l’API Provider assegna all’attributo «Livello di accesso» il valore Community o Restricted.
2. Richiesta di utilizzo delle API: Quando un soggetto richiede di poter utilizzare una API per realizzare una applicazione, l’Ecosistema invia all’API Provider una notifica di richiesta di utilizzo.

Si possono verificare due casi:

- Se il livello di accesso è «Community» E015 Digital Ecosystem considera da subito la richiesta come accettata (l’Ecosistema tiene traccia della relazione di utilizzo instaurata); l’API Provider - oltre a prender visione del soggetto e dell’applicazione utilizzatrice dell’API esposta - abilita il meccanismo di accesso all’API per la specifica applicazione richiedente entro 10 giorni lavorativi dalla data di richiesta;
- Se il livello è «Restricted», l’API Provider notifica all’Ecosistema l’accettazione o meno della richiesta e l’Ecosistema la propaga al soggetto richiedente; l’API Provider si impegna ad evadere le richieste di utilizzo delle proprie API entro 10 giorni lavorativi dalla data di richiesta; in caso di accettazione, l’Ecosistema tiene traccia della relazione di utilizzo instaurata e l’API Provider abilita il meccanismo di accesso all’API per la specifica applicazione richiedente, entro 10 giorni lavorativi dalla data di richiesta.

In entrambi i casi, l’API Provider dovrà procedere alle attività tecniche di configurazione necessarie per consentire a run-time l’accesso all’API a tutti i soggetti autorizzati.

Linee guida tecnologiche per la gestione dell’accesso alle API (meccanismo di attestazione)

Il meccanismo di attestazione si basa sia sull’utilizzo di token (es. token generati nell’ambito dell’adozione dello standard OAuth2.0, SAML, API Key, Basic Authentication, …) sia sull’uso di certificati X.509 (http://www.itu.int/rec/T-REC-X.509/en), resi disponibili attraverso i registri ufficiali dell’Ecosistema.

Di seguito vengono riportati i passi che l’API Provider deve eseguire al fine di adottare il meccanismo di attestazione tramite certificati X.509:

- Fase di descrizione e pubblicazione dell’API:
    - L’API Provider crea una coppia di chiavi: una privata e una pubblica inserita in un certificato X.509, ottenendola da una authority esterna o auto generandola. L’API Provider referenzia la chiave pubblica (certificato X.509) nel descrittore della propria API (attributo “Certificato X.509”);
    - L’API Provider configura il proprio application server su cui viene eseguita l’API (ed eventualmente – se necessario – i propri apparati di rete) per l’utilizzo della chiave privata inserendola nel relativo keystore in modo da realizzare un endpoint HTTPS sul quale ricevere le richieste di utilizzo; lo stesso endpoint deve essere configurato per richiedere al client di presentare il proprio certificato.
- Fase di gestione delle richieste di utilizzo**:**
    - Una volta ricevuta tramite l’Ecosistema, e approvata, nel caso di API «Restricted», una richiesta di utilizzo da parte di un soggetto fruitore, l’API Provider ottiene il certificato dell’applicazione. Tale certificato è inviato all’API Provider da parte dell’Ecosistema contestualmente alla richiesta di utilizzo dell’API.
    - L’API Provider inserisce il certificato del soggetto fruitore nel trust-store dell’application server su cui viene eseguita l’API. La modalità con cui svolgere questa attività dipende dai componenti sistemistici specifici utilizzati

dal singolo API Provider. In generale comunque, dal momento che ad ogni applicazione è associata una certificate chain, si potrà alternativamente:

- inserire nel truststore il certificato foglia della certificate chain;
- inserire nel truststore il certificato CA della certificate chain, configurando i propri appliance con regole specifiche per abilitare soltanto lo specifico certificato foglia (ad esempio, effettuando un controllo sul campo CN del certificato foglia associato a tale CA).

Queste due alternative sono del tutto equivalenti dal punto di vista concettuale di gestione del meccanismo di attestazione; l’API Provider può decidere autonomamente quale perseguire in base alle specificità dei propri componenti hardware per la gestione delle connessioni SSL.

- Fase di erogazione del API a runtime
  - Una volta ricevuta una richiesta applicativa da parte di una App, l’application server dell’API verifica in automatico che il certificato presentato sia tra quelli presenti nel proprio truststore / sia firmato da parte di una delle CA presenti nel proprio truststore.
  - Se la verifica va a buon fine, l’application server instaura con il fruitore un canale di comunicazione sicuro (SSL/TLS con Client Authentication) e rende disponibile al livello applicativo il certificato del fruitore per consentire l’attuazione delle eventuali politiche di autorizzazione.

I certificati delle API, al fine di essere compatibili con E015 Digital Ecosystem, devono possedere una struttura conforme ai requisiti che seguono:

- Durata: maggiore o uguale a 2 anni;
- Basic Constraint: End Entity (quindi non-CA);
- Key Usage (critical): Digital Signature e Key Encipherment;
- Enhanced Key Usage: Server Authentication, Client Authentication;
- Signature Algorithm: almeno sha256RSA per massimizzare la compatibilità con il software esistente.

È consentito l’utilizzo di certificati multi-dominio nel caso si debba utilizzare un singolo certificato per domini/API diversi (che rimangono comunque univocamente identificati da certificato e domain name). Questi certificati, denominati certificati ‘SAN’, riportano nel campo Subject Alternative Names l’elenco dei nomi di dominio per i quali il certificato deve essere considerato valido. Questo elenco viene definito al momento della creazione del certificato X509 indicando l’utilizzo dell’estensione ‘Subject Alternative Name’ e specificato come contenuto del campo Subject Alternative Name la lista di stringhe con l’elenco dei domini da considerare, nel seguente formato: ‘DNS:<domainName1>, DNS:<domainName2>’ (per maggiori dettagli si veda http://tools.ietf.org/html/rfc2818).

Il Technical Management Board presiede i processi per la gestione del meccanismo di attestazione:

- validando i certificati delle API all’atto della sottomissione del descrittore per approvazione;
- monitorando periodicamente la validità dei certificati pubblicati nei registri dell’Ecosistema e notificando agli API Provider la necessità di procedere al rinnovo in prossimità delle date di scadenza.

Si precisa che il ruolo di E015 Digital Ecosystem nella gestione del meccanismo di attestazione non è quello di emettere dei certificati, bensì quello di gestire l’albo ufficiale dei certificati delle API. Ciascun soggetto è libero infatti di decidere se acquisire i certificati X.509 da una authority esterna oppure se auto generarli [2].

Linee guida tecnologiche per la gestione degli aspetti di sicurezza delle API

Gestire la sicurezza nelle interazioni applicative tra API ed applicazioni di E015 Digital Ecosystem significa:

- fornire agli API provider opportuni strumenti per garantire proprietà dell’interazione quali: integrità e confidenzialità dei dati, prova della fonte, non ripudio ecc.;
- dare la possibilità agli API Provider di specificare i requisiti di sicurezza per l’accesso alle API erogate nell’Ecosistema.

I principali aspetti da considerare sono:

- gli strumenti per realizzare la sicurezza nelle interazioni applicative tra API;
- gli strumenti per permettere agli API Provider di specificare i requisiti di sicurezza delle proprie API.

Sicurezza e API SOAP

Per quanto riguarda la realizzazione di API sicure, nel contesto dell’Ecosistema si fa riferimento in generale allo stack tecnologico dei Web API e al WS-I Basic Security Profile 1.1.

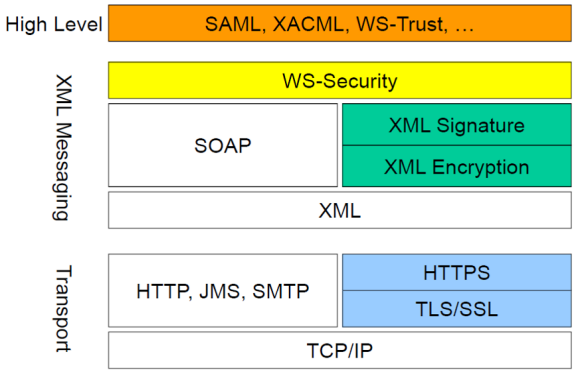

Figura 2.4: WS-Stack e tecnologie di sicurezza

In particolare, il WS-I Basic Security Profile 1.1 definito dalla OASIS WS-I Organization (http://www.oasis-ws-i.org/) indica le specifiche tecnologie da utilizzare con riferimento alle dimensioni di interoperabilità relative alla sicurezza e al trasporto in ambito Web Service SOAP.

Figura 2.5: WS-I Basic Security Profile 1.1 e tecnologie considerate

Lo standard OASIS WS-Security: SOAP Message Security (http://docs.oasis-open.org/wss/v1.1/) definisce diverse estensioni al protocollo SOAP al fine di garantire la protezione end-to-end dei messaggi scambiati nelle interazioni tra Web API SOAP. In particolare, i tre principali meccanismi forniti dallo standard sono:

- la possibilità di veicolare token di sicurezza come parte di un messaggio SOAP;
- la tutela dell’integrità del messaggio SOAP;
- la tutela della confidenzialità del messaggio SOAP.

Alla base di WS-Security c’è il concetto di security token: costrutti che possono essere usati all’interno dei messaggi SOAP (in particolare nell’header) per rappresentare e veicolare informazioni (per esempio di identità, oppure relative ai meccanismi di processing da eseguire per validare i token stessi). Lo standard WS-Security permette di usare diversi tipi di token: binari, basati su XML (tra cui rientrano le asserzioni SAML), criptati e altri ancora. Per la protezione di integrità e confidenzialità, WS-Security utilizza standard come XML-Signature e XML-Encription, applicandoli a determinate parti del messaggio SOAP.

In aggiunta al WS-I Basic Security Profile 1.1, per permettere agli API Provider di specificare i requisiti di sicurezza delle proprie API si considerano i seguenti standard:

- WS-Policy (http://www.w3.org/TR/ws-policy/) definisce un framework e un modello per rappresentare le policy di sicurezza di una API mediante descrizioni machine-readable: una policy può ad esempio descrivere i requisiti di sicurezza (autenticazione, autorizzazione ecc.) che il richiedente deve soddisfare per poter accedere a un API, oppure la messa in atto da parte dell’API Provider di determinati meccanismi come il tracciamento dei messaggi applicativi. Per esempio, tramite una policy WS-Policy un Web API può comunicare di essere in grado di accettare asserzioni SAML 2.0. WS-Policy

non entra nel merito della rappresentazione delle caratteristiche di una API: a tal fine possono essere usate altre specifiche, per esempio WS-SecurityPolicy.

- WS-SecurityPolicy (http://www.oasis-open.org/standards#ws-secpol) definisce le modalità di rappresentazione delle specifiche capacità o degli specifici requisiti di sicurezza di una API. Per esempio, grazie a WS-SecurityPolicy, è possibile scrivere una policy assertion per richiedere la presenza di un determinato elemento nell’header del messaggio SOAP.

I requisiti di sicurezza di un API così descritti possono diventare parte integrante del descrittore del API.

Sicurezza e API REST

Per le API REST in generale non esistono standard specifici per la gestione della sicurezza. Nell’ambito di E015 Digital Ecosystem è raccomandato l’utilizzo delle strategie e meccanismi di sicurezza comunemente utilizzate per l’accesso a web application (sicurezza di canale con SSL/TLS ecc.). Il Technical Management Board si riserva di accettare meccanismi di autenticazione differenti, purché adeguatamente documentati.

Glossari delle API

Gli aspetti relativi ai glossari all’interno del descrittore delle API

Si riportano nella tabella seguente i campi del descrittore delle API che indirizzano direttamente gli aspetti legati all’interoperabilità delle API.

Campo	Descrizione
Usi di glossari condivisi	Riferimento ad eventuali glossari condivisi dell’Ecosistema utilizzati da parte delle API

Linee Guida per la gestione dei glossari all’interno dell’Ecosistema

Un primo importante aspetto che indirizza la gestione dei Glossari all’interno dell’Ecosistema riguarda il modello dei dati di una API. Il modello dei dati di una API identifica e descrive:

- le entità e i concetti utilizzati nell’interazione con entità esterne per l’erogazione di funzionalità;
- la rappresentazione di tali entità e concetti (per esempio le modalità di serializzazione in costrutti XML da utilizzare nei messaggi di richiesta e risposta).

Pertanto è opportuno che il modello dei dati delle API dell’Ecosistema sia adeguatamente documentato, formalizzato e strutturato:

- la documentazione può consistere in una descrizione testuale (eventualmente guidata da un template comune);
- la formalizzazione può consistere in una rappresentazione dei concetti mediante opportuni linguaggi di descrizione (diagrammi UML http://www.uml.org/ , E-R ecc.);
- la strutturazione è la rappresentazione basata su una specifica tecnologia (per esempio un linguaggio di markup come XML) utilizzata dalla specifica API o applicazione.

1 Anche in questo caso, è necessario che l’API provider comunichi all’Ecosistema l’avvenuta revoca dell’accesso.

2 In generale è auspicabile l’acquisizione dei certificati presso authority esterne; al fine di garantire l’inclusività di un ampio numero di soggetti, E015 – Digital Ecosystem consente comunque l’uso di certificati auto generati.

Se adeguatamente descritti, formalizzati, strutturati e condivisi, i modelli dei dati abilitano il riuso nell’ambito di E015 Digital Ecosystem; diverse API e applicazioni infatti spesso utilizzano nel proprio modello dei dati gli stessi concetti, dunque:

- potrebbe essere già disponibile una rappresentazione degli stessi concetti;
- rappresentazioni di nuovi concetti potrebbero essere condivise con altri provider dell’Ecosistema.

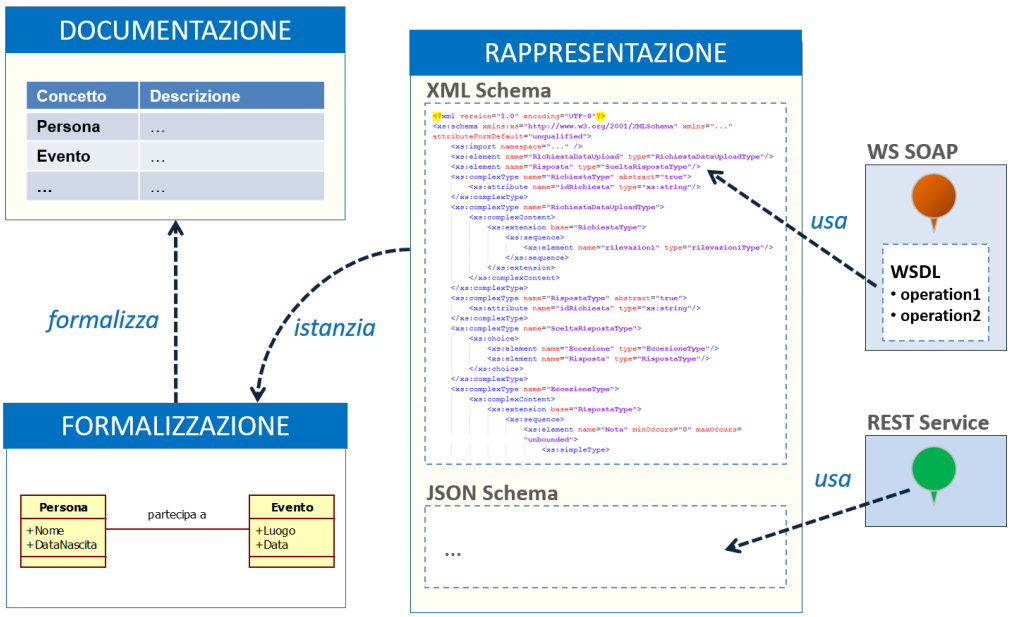

Figura 2.6: Modello dei dati: documentazione, formalizzazione, rappresentazione e utilizzo

L’approccio indicato per E015 Digital Ecosystem propone e incentiva l’adozione di glossari condivisi per favorire l’interoperabilità e il riuso nella realizzazione di API e delle applicazioni da parte dei soggetti aderenti all’ecosistema, difatti:

- I glossari condivisi permettono sia di classificare le API che di adottare modelli dei dati comuni;
- I glossari condivisi possono rappresentare un patrimonio informativo utilizzabile;
- È di interesse il potenziale ruolo degli operatori di dominio e/o delle associazioni di categoria per la definizione e l’evoluzione dei glossari;
- È importante promuovere l’inclusione nell’ecosistema di glossari e standard già esistenti in alcuni settori.

Condivisione e riuso di un modello dei dati possono avvenire a diversi “livelli” di specializzazione: i glossari infatti possono coprire concetti generali (tempo, geo-localizzazione ecc, concetti di specifici domini applicativi (turismo, trasporti, enogastronomia, alberghiero ecc.), concetti specifici di una singola applicazione o di una singola API.

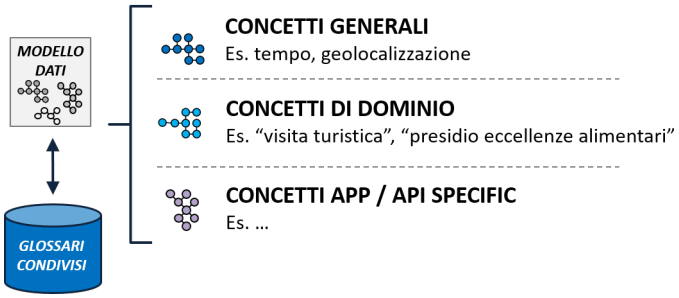

Figura 2.7: Possibili livelli di specializzazione di un glossario

Inoltre, i glossari condivisi possono essere più o meno formalizzati: da semplici tag, keyword o vocabolari si può arrivare a tassonomie complete o ad una vera e propria formalizzazione in ontologie. In fase di sottomissione di una nuova API da pubblicare all’interno dell’Ecosistema il TMB verificherà l’eventuale presenza di glossari già disponibili e di potenziale interesse per l’API Provider, rispetto ai quali rendere coerente l’interfaccia ad il modello dei dati dell’ API stessa.

Aspetti relativi al monitoraggio delle API

Gli aspetti relativi al monitoraggio all’interno del descrittore delle API

Si riportano nella tabella seguente i campi del descrittore delle API che indirizzano direttamente gli aspetti legati all’interoperabilità delle API.

Campi del descrittore relativi al monitoraggio

Campo	Descrizione
Endpoint di monitoraggio	Endpoint per il controllo di disponibilità dell’API
Invocazioni di test per monitoraggio	Formulazione delle invocazioni di test da utilizzare per la verifica di disponibilità dell’API e per la verifica della correttezza delle risposte ottenute.
Frequenza di monitoraggio	Indicazione da parte dell’API Provider di una frequenza di monitoraggio compatibile col tipo di API erogata per quello specifico dominio.
Segnalazioni specifiche	Opzionale: es. down quotidiani programmati per attività di manutenzione

L’approccio dell’Ecosistema per il monitoraggio delle API

In generale è di interesse per l’Ecosistema poter verificare su base continuativa se le API sono attive e come/quanto queste vengono usate da parte delle applicazioni. Per questo motivo, l’Ecosistema prevede dei meccanismi di base per il monitoraggio continuativo delle API pubblicate; in particolare, a partire dalla versione 1 verrà effettuato un controllo di disponibilità delle API. Al fine di consentire a E015 Digital Ecosystem di poter effettuare tale controllo, l’API Provider è tenuto a specificare all’interno del descrittore dell’API un endpoint di monitoraggio e ad esprimere una frequenza di monitoraggio compatibile con il tipo di API erogata. Inoltre l’API Provider deve fornire all’interno del descrittore anche delle invocazioni “campione” di test (request e response), le quali saranno utilizzate dall’Ecosistema per la verifica di disponibilità dell’API e per la verifica della correttezza delle risposte ottenute.

L’Ecosistema utilizza l’endpoint di monitoraggio specificato nel descrittore per controllare periodicamente l’effettiva disponibilità dell’API (attraverso un semplice meccanismo di “ping”) e per effettuare delle invocazioni di test sulla base delle invocazioni “campione” specificate dall’API provider all’interno del descrittore.

Da un punto di vista operativo, la gestione degli aspetti di monitoraggio delle API erogate impatta su due fasi specifiche del processo di pubblicazione e di erogazione delle API:

1. Descrizione dell’API: In fase di compilazione del descrittore dell’API, l’API Provider compila gli attributi: “Endpoint di monitoraggio”, “Invocazioni di test per monitoraggio” e “Frequenza di monitoraggio” (utilizzati dall’Ecosistema per effettuare il controllo di disponibilità e di correttezza delle risposte delle API), “Messaggi di indisponibilità” (opzionale), “Test suite” (opzionale) , “Endpoint ambiente di test” (opzionale) e “Segnalazioni specifiche” (opzionale).
2. Erogazione dell’API: A run-time E015 Digital Ecosystem effettua periodicamente il controllo di disponibilità delle API e verifica la correttezza delle risposte ricevute in seguito alle invocazioni campione specificate nel descrittore. Il monitoraggio è effettuato “ai morsetti esterni” del API, poiché indica il livello di disponibilità con cui è percepito l’API dall’Ecosistema.

Il TMB utilizza i dati di monitoraggio per comprendere il livello di qualità dell’API erogata (in termini di disponibilità) e in seguito restituire tale informazione all’API Provider, nonché diffondere l’andamento del monitoraggio alle applicazioni che utilizzano l’API esposta.

Aspetti correlati all’erogazione di una API

Gli aspetti relativi all’erogazione all’interno del descrittore dell’ API

Si riportano nella tabella seguente i campi del descrittore dell’API che indirizzano direttamente gli aspetti legati all’erogazione dell’API.

Campi del descrittore relativi all’erogazione dell’API

Campo	Descrizione
Impegni/capacità di erogazione	Indicazione generale su base volontaria della capacità di erogazione dell’API che l’API Provider indica di poter sostenere nei confronti dell’Ecosistema (secondo una logica best effort).

Logiche di remunerazione	Indicazione della logica di remunerazione connessa all’erogazione dell’API. I valori ammissibili per questoattributo del descrittore sono: 1. Free: per API che non prevedono alcuna forma di tariffazione; 2. A pagamento: per API che prevedono il pagamento di una tariffa legata all’utilizzo. Modelli di tariffazione supportati (attributo specifico da compilare per le sole API “a pagamento”): Indicazione dei modelli supportati per la tariffazione di API a pagamento. Tipologia di QoS supportate (attributo specifico da compilare per le sole API “a pagamento”): Indicazione delle tipologie di API level sulle quali l’API Provider si rende disponibile a stipulare accordi puntuali con specifici utilizzatori delle API.
Dimensionamento dei flussi informativi	Informazioni circa le dimensioni dei flussi informativi in ingresso e in uscita dall’API.

Impegni / capacità di erogazione

E015 Digital Ecosystem prevede che normalmente le API siano erogate secondo una logica di tipo Best effort; è interesse degli API Provider erogare verso l’Ecosistema API di qualità al fine di incentivare un ampio utilizzo delle stesse da parte delle applicazioni. All’interno del descrittore il campo “Impegni / capacità di erogazione” offre all’API Provider la possibilità di comunicare all’Ecosistema, su base volontaria, le disponibilità e gli impegni di massima che esso si rende disponibile a sostenere per l’erogazione della propria API; ad esempio, l’API Provider può dichiarare all’interno del descrittore – relativamente al campo “Impegni / capacità di erogazione” – il numero massimo di invocazioni giornaliere per Applicazione supportate dalla propria API. Tali informazioni rappresentano una utile indicazione verso il TMB per favorire l’ottimizzazione dell’utilizzo dell’API da parte delle applicazioni - sempre e comunque in una logica complessiva di tipo best effort [3] - e per promuovere il miglioramento progressivo nel tempo della qualità delle funzionalità esposte.

Logiche di remunerazione

Ciascun soggetto dell’Ecosistema ha la possibilità di perseguire proprie logiche di remunerazione legate all’erogazione delle API. È pertanto possibile che gli API Provider decidano di erogare le proprie API solo a soggetti con i quali è stato definito un accordo di tipo commerciale.

Al fine di dare evidenza di questa possibilità, gli API Provider devono specificare all’interno del descrittore se le proprie API sono disponibili a pagamento (attributo “Logiche di remunerazione”). In questo modo, E015 Digital Ecosystem facilita la stipulazione di accordi commerciali tra le diverse parti. All’interno del descrittore, relativamente all’attributo “Logiche di remunerazione”, sarà possibile selezionare pertanto una delle seguenti opzioni:

1. Free: non è prevista alcuna forma di tariffazione; l’API è erogata gratuitamente ai soggetti autorizzati ad accedervi;
2. A pagamento: l’accesso all’API è soggetto a tariffazione.

Nel caso di API “a pagamento”, l’API Provider è tenuto a compilare anche i campi del descrittore “Modelli di tariffazione supportati”, “Tipologie di QoS supportate” e “Referente commerciale” al fine di indicare gli aspetti di interesse sulla base dei quali la tariffa di erogazione dell’API sarà concordata.

Si precisa che nel caso di API “a pagamento” la negoziazione della tariffa tra API Provider e i soggetti utilizzatori avviene al di fuori dell’Ecosistema. Qualora l’API Provider desiderasse esporre all’interno dell’Ecosistema due versioni della medesima API, una “free” ed una “a pagamento” - per l’utilizzo della quale è necessario stipulare un accordo di tipo commerciale - è necessario procedere alla pubblicazione di due API distinte, ciascuna delle quali corredata da un proprio descrittore specifico.

Modelli di tariffazione supportati (API “a pagamento”)

Nel caso di API “a pagamento” l’API Provider deve specificare all’interno del descrittore, nel campo “Modelli di tariffazione supportati”, quali sono le modalità previste per il riconoscimento di un corrispettivo economico derivante dall’utilizzo dell’API da parte delle applicazioni. Esempi di modelli di tariffazione che possono essere specificati all’interno di questo campo sono: pagamento una tantum, pagamento di un abbonamento, pagamento a consumo, pagamento in base alla QoS garantita ecc.

Tipologie di QoS supportate (API “a pagamento”)

Nel caso di API “a pagamento” per i quali sia previsto un modello di tariffazione basato su garanzie di qualità (QoS), è necessario che l’API Provider compili il campo del descrittore “Tipologie di QoS supportate”.

All’interno di questo campo l’API Provider dichiara le tipologie di API level sulla base delle quali esso è disponibile a definire la tariffa di erogazione dell’API (stipulando in questo modo accordi di tipo commerciale). Esempi di possibili tipologie di API level sono: disponibilità dell’API, response time, volume di traffico per tipologia di transazioni campione, soglie di traffico, fasce orarie di erogazione ecc.

Dimensionamento dei flussi informativi

Al fine di consentire ai soggetti utilizzatori di ottimizzare l’utilizzo delle API dell’Ecosistema, è data facoltà agli API Provider di fornire, nel campo “Dimensionamento dei flussi informativi”, alcune indicazioni circa le dimensioni (ad esempio, in kb) dei flussi informativi in ingresso e in uscita dall’API in corrispondenza di invocazioni campione rappresentative di un normale utilizzo.

Aspetti legati all’azienda erogatrice delle API

Si riportano nella tabella seguente i campi del descrittore dell’API che indirizzano direttamente gli aspetti legati all’azienda erogatrice dell’API.

Gli aspetti relativi all’azienda all’interno del descrittore dell’ API

Campi del descrittore relativi all’azienda erogatrice dell’API

Campo	Descrizione

Descrittore dell’API

Anagrafica dell’API	Attributi di descrizione anagrafica dell’API: 1. Nome dell’ API: nome univoco dell’API all’interno dell’Ecosistema. 2. Descrizione dell’API: descrizione sintetica in testo libero dell’API, la quale fornisce una presentazione funzionale dell’API. 3. Versione del descrittore: indicazione della versione del descrittore. 4. Tag per classificazione dell’API: insieme di parole chiave che consentono di classificare l’API. 5. Eventuali ulteriori vincoli specifici: in ingresso e in uscita dall’API. ventuali ulteriori vincoli che è eventuali ulteriori vincoli che è necessario conoscere / rispettare per utilizzare l’API. 6. Estensione geografica contenuti dell’API: indicazione dell’estensione geografica dei dati restituiti dalla API(utile a favorirne la ricerca)

Linee Guida per la gestione degli aspetti relativi all’azienda

Il descrittore dell’API rappresenta uno strumento fondamentale non solo per documentare gli aspetti di tipo tecnologico legati all’erogazione di una API, ma anche per indirizzare tematiche di tipo organizzativo e di relazione tra l’API Provider e l’Ecosistema.

Per questo motivo, all’interno del descrittore devono essere indicati:

- i principali attributi di tipo anagrafico dell’API (nome API, descrizione, nome API provider, versione, tag per classificazione ecc.), importanti al fine di consentire una comprensione generale dell’API anche da parte di interlocutori non tecnici; tali attributi hanno una valenza importante anche a scopo di comunicazione (alcuni attributi di anagrafica delle API saranno infatti resi visibili pubblicamente sui registri di E015 Digital Ecosystem anche da parte di soggetti non aderenti all’iniziativa); in particolare, la descrizione dell’API fornita all’interno del descrittore deve consentire di comprendere al meglio le caratteristiche funzionali dell’API ed il valore potenziale per i soggetti che ne intendono fare uso;
- i riferimenti (nome, cognome, e-mail, numero di telefono) del referente dell’API nei confronti dell’Ecosistema. Tale referente deve avere compreso a pieno le logiche di E015 Digital Ecosystem e deve essere il punto di contatto per il TMB qualora vi fosse la necessità di indirizzare alcune tematiche di interesse legate all’erogazione dell’API. Le informazioni relative al referente dell’API non saranno rese visibili agli App Provider, ma sono da intendersi ad uso esclusivo del TMB.

---

3 Si precisa che le dichiarazioni riportate nel campo “Impegni / capacità di erogazione” hanno carattere puramente indicativo e non rappresentano un vincolo per l’ API Provider.

Linee Guida per la pubblicazione sul proprio sito web istituzionale delle informazioni sulle API di E015 Digital Ecosystem

Una volta pubblicato una API all’interno dell’Ecosistema, l’API Provider deve prevedere sul proprio sito web istituzionale una sezione dedicata alla descrizione dell’iniziativa di partecipazione all’Ecosistema e alla descrizione delle API pubblicate con un link che rimanda al sito web dell’Ecosistema, per il dettaglio delle informazioni delle API pubblicate.

La presenza o meno di tali informazioni all’interno del sito web istituzionale del API Provider sarà oggetto di verifica da parte del TMB e rappresenterà un aspetto di interesse ai fini dell’accettazione o meno della richiesta di pubblicazione di una nuova API.

Ciclo di vita di una API (API lifecycle)

Si riportano nella tabella seguente i campi del descrittore dell’API che indirizzano direttamente gli aspetti legati al ciclo di vita dell’API.

Gli aspetti relativi al lifecycle all’interno del descrittore dell’API

Campi del descrittore relativi all’API lifecycle

Campo	Descrizione
Versione dell’API	Identificativo della versione dell’API all’interno dell’Ecosistema.
Riferimento ad altre versioni dell’API altre versioni dell’API	Riferimento ad eventuali altre versioni dell’API pubblicate all’interno dell’ Ecosistema. Per ogni riferimento viene fornito un changelog delle diverse versioni.

Il ciclo di vita delle API di E015 Digital Ecosystem

Le API di E015 Digital Ecosystem rappresentano dei “building-block” riusabili messi a disposizione degli App provider per le realizzazione delle applicazioni.

Al fine di consentire l’erogazione di applicazioni di qualità è importante che:

- L’API Provider comunichi Major Change non retrocompatibili (cambio tracciato dati, cambio policy, dismissione dell’API) con almeno 6 mesi di preavviso. In questo modo, chi realizza le applicazioni ha la garanzia del periodo temporale nel corso del quale le API utilizzate saranno effettivamente erogate con continuità.
- Le API pubblicate nell’Ecosistema siano il più possibile stabili, non solo da un punto di vista tecnico, ma anche e soprattutto da un punto di vista della continuità del “business”; un’API nata per esigenze temporanee e che molto probabilmente verrà dismessa nel giro di qualche mese può provocare un significativo impatto sulle applicazioni che ne fanno uso; per questo motivo non potrà essere pubblicata all’interno di E015 Digital Ecosystem, non essendo considerata “stabile”, ovvero non potendo garantire un significativo orizzonte temporale di erogazione.

Al fine di soddisfare questi importanti requisiti è necessario che tutte le API dell’Ecosistema siano erogate in accordo al “lifecycle” descritto nel seguito:

1. una volta valutata positivamente l’opportunità di pubblicare una API all’interno dell’Ecosistema, l’ API Provider compila il descrittore dell’ API;
2. successivamente alla pubblicazione e all’approvazione del descrittore da parte del TMB, l’API entra nella fase di “erogazione”. Durante questa fase l’API Provider si impegna a

mantenere attiva la propria API con continuità, in modo da consentirne un utilizzo prolungato nel tempo da parte delle applicazioni;

3. Nel caso di Major Change non retrocompatibili (fra le quali cambio di policy o dismissione), l’API Provider è tenuto a comunicarlo con un prevviso di 6 mesi. Nell’arco di questi 6 mesi l’API Provider si impegna a mantenere stabile la versione in dismissione. Questa fase consente agli App Provider di poter intervenire sulla proprie applicazioni
4. Una volta effettivamente esaurito il transitorio di 6 mesi può verificarsi una delle seguenti situazioni:

    - l’API viene definitivamente dismessa e le applicazioni non ne possono più fare uso;
    - è stata nel frattempo pubblicata una nuova versione dell’API e l’Ecosistema invia alle applicazioni utilizzatrici una notifica nella quale promuove la migrazione verso la nuova versione;
    - l’Ecosistema invia alle applicazioni utilizzatrici una notifica nella quale comunica che l’API sarà ancora disponibile.

Generalmente non è possibile dismettere una API prima dei sei mesi, ad eccezione dei seguenti casi:

1. l’API non risulta più in utilizzo da parte di alcuna applicazione (ad esempio, perché tutte le applicazioni utilizzatrici hanno effettuato una migrazione ad una successiva versione);
2. eventuali cause di forza maggiore.

Dal momento che le API di E015 Digital Ecosystem possono essere soggette ad evoluzioni, è necessario prevedere la possibilità da parte dell’API Provider di pubblicare molteplici versioni di una stessa API.

Le linee guida per la pubblicazione di una nuova versione dell’API sono le seguenti:

1. le evoluzioni dell’API che comportano modifiche di Major Change non retrocompatibili determinano la pubblicazione di nuove versioni tra loro indipendenti. In questo caso:

    - le nuove versioni di una API devono essere erogate tramite un endpoint dedicato e il loro processo di pubblicazione segue il normale iter previsto per la pubblicazione di una nuova API (in particolare, il campo “Riferimento ad altre versioni dell’API” referenzierà le versioni precedenti);
    - le versioni precedenti dell’API continuano ad essere attive e restano a disposizione delle applicazioni, come indicato in Figura 2.8. È possibile pertanto che più versioni della stessa API, le quali differiscono tra loro a livello di interfaccia e/o modello dei dati, siano attive contemporaneamente;
    - l’Ecosistema notifica alle applicazioni utilizzatrici la disponibilità di una nuova versione dell’API, promuovendo la migrazione alla versione più recente.

2. Le evoluzioni dell’API che NON comportano modifiche all’interfaccia (ad esempio, che determinano un incremento della qualità dei dati erogati) non necessitano della pubblicazione di una nuova versione indipendente. In questo caso le modifiche all’API – previa approvazione da parte del TMB – vengono eseguite direttamente sulla stessa istanza dell’API già pubblicata all’interno dell’Ecosistema. L’Ecosistema provvede ad inviare delle notifiche ai soggetti utilizzatori, specificando le caratteristiche dell’API oggetto di evoluzione.

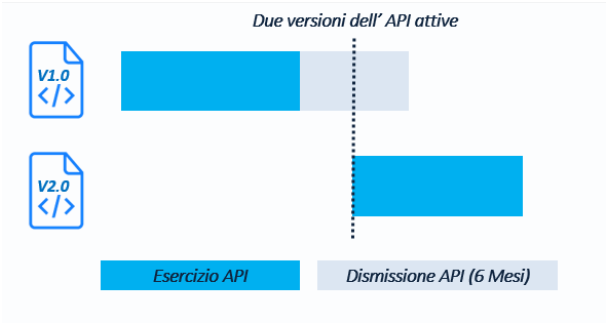

Figura 2.8: Gestione delle versioni delle API in E015 Digital Ecosystem

Policies delle API

Gli aspetti relativi alle policy all’interno del descrittore dell’API

Si riportano nella tabella seguente i campi del descrittore dell’API che indirizzano direttamente gli aspetti legati all’interoperabilità delle API.

Campi del descrittore relativi all’API lifecycle

Campo	Descrizione
Policy generale di utilizzo	Riferimento al documento contenente le condizioni di utilizzo dell’API valide per tutti i soggetti utilizzatori.

Approccio dell’Ecosistema per la gestione delle policy delle API

E015 Digital Ecosystem prevede che ogni API Provider stabilisca quali condizioni di utilizzo delle API i soggetti debbano impegnarsi a rispettare. In particolare, è necessario che per ciascuno delle proprie API pubblicate l’API Provider specifichi all’interno del descrittore le relative Policy generali di utilizzo.

Tali policy indicano le condizioni di utilizzo dell’API comuni per tutti gli App Provider e devono essere accettate da parte di ogni soggetto utilizzatore che intende utilizzare la specifica API. Se non rispettate, possono comportare l’inibizione da parte dell’API provider dell’accesso alla propria API.

In generale i soggetti aderenti godono della massima autonomia nella definizione di dettaglio di queste policy; il TMB fornisce un supporto indicando eventualmente possibili modelli di riferimento o segnalando eventuali situazioni che comportano un potenziale ridotto utilizzo delle API esposte. Esempi di possibili elementi contenuti all’interno delle policy generali / specifiche di utilizzo sono:

- Proprietà dei dati erogati dalle API.
- Possibilità di manipolare e/o modificare i dati erogati dalle API.
- Clausole per l’utilizzo e la visualizzazione parziale dei dati erogati dall’API.
- Clausole relative all’aggiornamento delle informazioni (Es: obbligo di mostrare agli utenti l’ora di aggiornamento).
- **Eventuale riferimento a framework di licensing già esistenti. Ad esempio:** Creative Commons

    - Italian Open Data License.
    - …
- Clausole di esonero di responsabilità.
- Clausole in merito alla storicizzazione delle informazioni erogate dalle API.
- Eventuale riferimento al codice etico dell'API Provider.
- Clausole relative alla privacy e alla eventuale gestione di dati sensibili.
- Possibilità di visualizzare messaggi di tipo pubblicitario contestualmente alle informazioni erogate dalle API.
- **Obbligo di citare il soggetto erogatore delle informazioni:**
    - semplice citazione testuale;
    - utilizzo di un logo.
- Clausole relative ad eventuali sospensioni dell'erogazione dell'API.
- Altro

In Figura 2.9 è riportata una schematizzazione esemplificativa relativa a possibili framework di licensing già disponibili che gli API provider potrebbero decidere di referenziare e adottare all'interno delle proprie policy. Ad esempio:

1. per quanto concerne i contenuti erogati dalle API (file audio, immagini, video) è possibile utilizzare le licenze Creative Commons; nel caso in cui si volesse adottare un modello di licensing chiuso, gli API Provider possono decidere di proteggere i propri contenuti con diritti di copyright;
2. per quanto concerne i dati messi a disposizione (ad esempio, file corrispondenti a intere banche dati) è possibile utilizzare le licenze Open Data Commons; nel caso in cui si volesse adottare un modello di licensing chiuso, gli API Provider possono decidere di proteggere i propri dati con diritti di copyright;
3. per quanto concerne le API, è necessario definire all'interno delle Policy generali e all'interno delle Policy specifiche quali siano i Termini delle API previste.

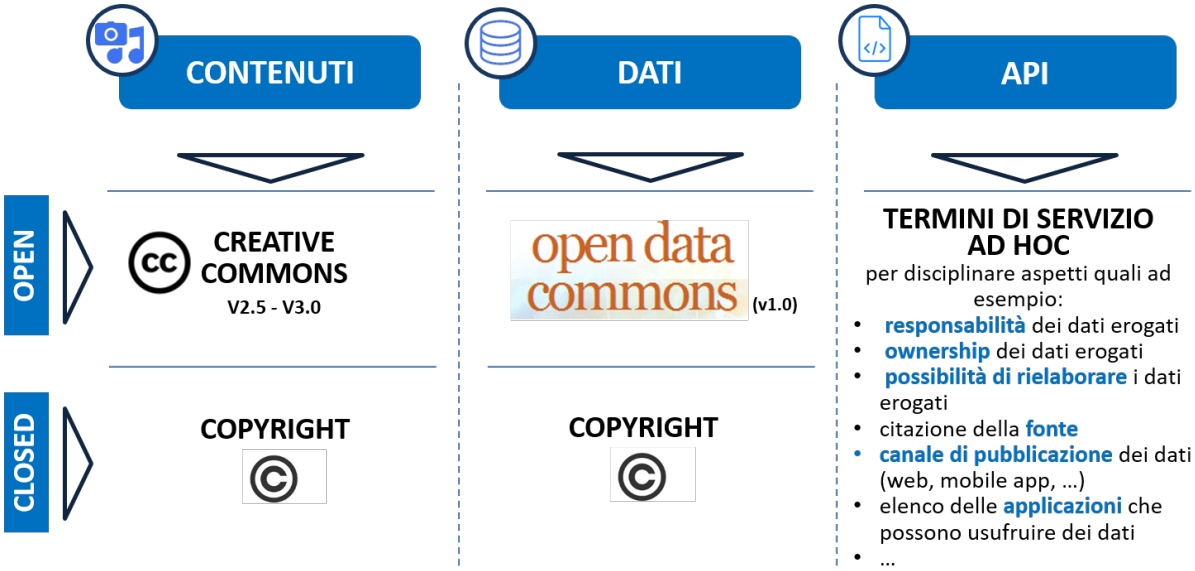

Figura 2.9: Esempi di modelli di licensing adottabili in E015 Digital Ecosystem

Verifiche del Technical Management Board per la pubblicazione delle API

Il processo di pubblicazione di una API all'interno di E015 Digital Ecosystem prevede che il Technical Management Board effettui le verifiche necessarie a garantire che le API pubblicate posseggano tutte le caratteristiche di validità richieste dall'Ecosistema.

Elementi di verifica da parte del Technical Management Board

Una volta ricevuta da parte dell'API Provider la richiesta di pubblicazione di una API, corredata dal descrittore dell'API compilato in ogni sua parte, il Technical Management Board procede ad eseguire le seguenti verifiche:

1. Verifica di completezza del descrittore: tutti gli attributi obbligatori devono essere valorizzati ed adeguatamente documentati.
2. Verifica della correttezza e della coerenza del descrittore: tutti gli attributi devono essere compilati coerentemente con le Linee Guida del presente documento.
3. Verifica di coerenza dell'API con le Linee Guida tecnologiche di E015 Digital Ecosystem: l'API deve rispettare tutte le indicazioni tecnologiche fornite in questo documento.
4. Test di invocazione dell' API: il TMB, attraverso opportuni strumenti, effettua delle invocazioni di test, verificando così il funzionamento dell'API e la consistenza del comportamento effettivo con quanto documentato all'interno del descrittore e della documentazione tecnica ad esso allegata. [4]
5. Verifica di disponibilità dell'API: il TMB "aggancia" l'API al componente core di verifica di disponibilità al fine di verificare gli aspetti specifici relativi al monitoraggio. Sulla base dell'esito di tali verifiche il TMB comunicherà all'API Provider l'accettazione della richiesta di pubblicazione dell'API; in caso di rifiutodella richiesta, il TMB fornirà all'API Provider le indicazioni di "non conformità" al fine di consentire la risoluzione delle problematiche riscontrate, la rimozione di eventuali ostacoli al fine di favorire la successiva pubblicazione dell'API.

Esito del processo di verifica

Come descritto nel paragrafo precedente, il processo di verifica delle API può concludersi positivamente o meno a seconda delle non conformità rilevate dal Technical Management Board in fase di verifica dell'API. In caso di esito positivo del processo di verifica, il Technical Management Board dell'Ecosistema rilascia all'API Provider un resoconto con il dettaglio delle verifiche svolte contenente una attestazione di conformità dell'API alle Linee Guida per la pubblicazione delle API definite nell'Ecosistema e descritte nelle sezioni precedenti. Questa attestazione di conformità formalizza l'accettazione da parte dell'Ecosistema della richiesta di pubblicazione dell'API precedentemente inviata dall'API Provider e riconosce al soggetto aderente il ruolo di API Provider dell'Ecosistema.

In caso di esito positivo del processo di pubblicazione, il Technical Management Board include l'API all'interno del registro ufficiale delle API dell'Ecosistema e procede ad integrarlo all'interno dell'ambiente di "preview" dell'API (tale ambiente di "preview" costituisce una particolare sezione del registro delle API all'interno della quale viene data una dimostrazione reale - attraverso una interfaccia grafica interattiva – delle funzionalità erogate dall'API).

Qualora durante la sessione di verifica dell'API fossero rilevate dal Technical Management Board delle non conformità (lievi e comunque non bloccanti) rispetto alle linee guida descritte nei paragrafi precedenti, il report finale riporterà anche una serie di raccomandazioni per le quali il Technical Management Board richiede la definizione di un piano di interventi da parte dell'API Provider per superare le non conformità rilevate [5].

[4] Al fine di consentire al TMB di poter effettuare queste verifiche, è necessario che l'API Provider configuri il meccanismo di restrizione dell'accesso all'API (meccanismo di attestazione) al fine di garantire l'accesso programmatico da parte del TMB. In particolare, l'API Provider dovrà includere all'interno del trust store associato al proprio API il certificato client del TMB reso disponibile dall'Ecosistema.

[5] La mancata definizione del piano di interventi per le singole raccomandazioni segnalate oppure il mancato rispetto dei tempi indicati nel piano di interventi definito dal API Provider può costituire motivo di revoca della pubblicazione del API all'interno dell'Ecosistema.