



UNIVERSITÀ
DEGLI STUDI
FIRENZE

Scuola di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Informatica

Tesi di Laurea

ESPRIMERE IN FACPL POLITICHE DI
CONTROLLO DEGLI ACCESSI BASATE SUL
COMPORTAMENTO PASSATO

EXPRESSING ACCESS CONTROL POLICIES
BASED ON PAST BEHAVIOR IN FACPL

FEDERICO SCHIPANI

Relatore: *Rosario Pugliese*
Correlatore: *Andrea Margheri*

Anno Accademico 2014-2015

INDICE

1	INTRODUZIONE	9
2	ACCESS CONTROL E USAGE CONTROL	11
2.1	Access Control	11
2.2	Usage Control	17
2.2.1	Caso di studio 1: Gestione lettura e scrittura di file	18
2.2.2	Caso di studio 2: Noleggio e acquisto di contenuti	19
3	FORMAL ACCESS CONTROL POLICY LANGUAGE	23
3.1	Il processo di valutazione di FACPL	24
3.2	La sintassi di FACPL	25
3.3	La semantica di FACPL	27
3.4	Esempio di politica con FACPL	29
4	IMPLEMENTARE USAGE CONTROL IN FACPL	33
4.1	Estensione del processo di Valutazione	33
4.2	Estensione Linguistica	36
4.3	Semantica	38
4.4	Esempi	42
4.4.1	Accesso ai file	42
4.4.2	Noleggio e acquisto di contenuti	46
5	ESTENSIONE DELLA LIBRERIA FACPL	51
5.1	Estensione delle classi	51
5.2	Status e Status Attribute	52
5.3	Implementazione dei comparatori sugli Status Attribute	55
5.4	Funzioni per la modifica degli Status Attribute	56
5.5	Estensione del contesto	60
5.6	Obligations e PEP	62
5.7	Plugin di Eclipse	65
5.8	Esempio	66
6	CONCLUSIONI	71
6.1	Futuro di FAPCL	71
A	CODICE COMPLETO	77
A.1	Capitolo 4	77
A.2	Capitolo 5	80

A.2.1	Status e Status Attribute	80
A.2.2	Implementazione dei comparatori sugli Status Attribute	82
A.2.3	Funzioni per la modifica degli Status Attribute	83
A.2.4	Obligations e PEP	86
A.2.5	Esempio	93

ELENCO DELLE FIGURE

Figura 1	ACL in OS X	13
Figura 2	Gruppo in OS X	14
Figura 3	Scenario ABAC base	15
Figura 4	Insieme dei componenti di $U\text{CON}_{ABC}$	18
Figura 5	Diagramma di flusso del primo esempio	19
Figura 6	Diagramma di flusso del secondo esempio	21
Figura 7	ToolChain di FACPL	23
Figura 8	Il processo di valutazione di FACPL	24
Figura 9	Nuovo processo di valutazione in FACPL	34
Figura 10	Grafico UML delle classi Status e StatusAttribute	53
Figura 11	Grafico UML per la gerarchia di classi usate nella comparazione	57
Figura 12	Grafico UML per la gerarchia di funzioni aritmetiche	58
Figura 13	Grafico UML del contesto	61
Figura 14	Relazioni tra Obligation e PEP	63
Figura 15	Logo di Xtend	66

LISTA DI CODICI

3.1	Esempio di politica in FACPL	29
3.2	Richieste per Codice 3.1	30
4.1	Esempio per la sintassi	37
4.2	Primo esempio	42
4.3	Richieste del primo esempio	44
4.4	Secondo Esempio	46
4.5	Secondo Esempio	47
4.6	Richieste del Secondo Esempio	48
5.1	Stralcio della classe Status	53
5.2	Metodi per gli <i>Status Attribute</i>	53
5.3	Costruttori di Status Attribute	54
5.4	Classe che implementa Equal	55
5.5	Interfaccia per le operazioni	56
5.6	Metodo implementato dall'interfaccia	56
5.7	Classe per la somma	59
5.8	Metodo implementato dall'interfaccia	60
5.9	Classe ContextStub_Default_Status	60
5.10	Parte rifattorizzata del metodo che si occupa del fulfilling	62
5.11	CreateObligation nelle status	64
5.12	CreateObligation nelle normali	64
5.13	Peculiarità della classe FulfilledObligationStatus	64
5.14	Discharge delle Fulfilled Obligation di stato	65
5.15	Main di uno scenario FACPL	66
5.16	Richiesta e contesto	67
5.17	Expression Function che valuta un attributo di stato	69
A.1	Secondo Esempio Completo	77
A.2	Stralcio della classe Status	80
A.3	Costruttori di Status Attribute	81
A.4	Classe che implementa Equal	82
A.5	Metodo implementato dall'interfaccia	83
A.6	Parte rifattorizzata del metodo che si occupa del fulfilling	86
A.7	CreateObligation nelle status	88

6 Lista di Codici

A.8 CreateObligation nelle normali	88
A.9 Discharge delle Fulfilled Obligation di stato	89
A.10 Policy StopRead	93
A.11 Policy StopRead	98

Ezechiele 25:17. "Il cammino dell'uomo timorato è minacciato da ogni parte dalle iniquità degli esseri egoisti e dalla tirannia degli uomini malvagi. Benedetto sia colui che nel nome della carità e della buona volontà conduce i deboli attraverso la valle delle tenebre, perché egli è in verità il pastore di suo fratello e il ricercatore dei figli smarriti. E la mia giustizia calerà sopra di loro con grandissima vendetta e furiosissimo sdegno su coloro che si proveranno ad ammorbare e infine a distruggere i miei fratelli. E tu saprai che il mio nome è quello del Signore quando farò calare la mia vendetta sopra di te."
— Jules Winnfield [Voce di Luca Ward]

"Stay hungry, stay hungry"
— Paolo Bitta, l'uomo chiamato contratto

INTRODUZIONE

I sistemi informatici si sono diffusi molto rapidamente, e grazie all'avvento di nuove tecnologie, come la rete, la condivisione di dati e risorse è diventata alla portata di tutti. Proteggere queste risorse da accessi indesiderati è diventato molto importante, motivo per cui negli ultimi decenni la questione del *Access Control* è diventata sempre più rilevante. In particolare, a partire dal 1970, sono stati proposti vari modelli (come Access Control List (ACL), Role Based Access Control (RBAC), Attribute Based Access Control (ABAC) e Policy Based Access Control (PBAC)), ognuno dei quali ha i suoi pro e contro.

Il primo modello proposto è ACL ed ha come obiettivo il controllo delle risorse di un sistema operativo. Questo modello si basa su liste di accesso associate ad ogni risorsa che definiscono le regole di accesso; è un modello molto semplice da implementare, ma quando i dati sono eccessivi diventa poco efficiente. Successivamente è stato introdotto un modello basato su ruoli chiamato RBAC, il quale associa a degli insiemi di risorse dei diritti di accesso, ovvero dei gruppi di utenti suddivisi secondo caratteristiche comuni. Un punto debole di questo modello è l'assenza di costrutti che permettono la definizione delle regole che rende difficile assegnare permessi particolari a singole risorse. A seguire è stato utilizzato un modello basato su attributi chiamato ABAC, dove le decisioni vengono prese valutando caratteristiche del richiedente, della risorsa e dell'ambiente in cui è stata fatta la richiesta. Quest'ultimo modello tuttavia non offre una buona scalabilità. Per porre rimedio a questo difetto è stato introdotto un ulteriore modello, che si chiama PBAC il quale risulta essere uno dei più utilizzati ed è basato su politiche, ovvero un insieme di regole su attributi.

Recentemente, Sandhu e Park [5] hanno introdotto *Usage Control* che permette di prendere decisioni durante l'accesso e di basarsi sul comportamento passato in fase di valutazione di una richiesta. Questa caratteristica lo rende molto adatto ad ambienti come il Web, il Cloud o in generale

legati in qualche modo alla rete.

Formal Access Control Policy Language (FACPL) è un linguaggio basato su eXtensible Access Control Markup Language (XACML), supportato da una libreria scritta in Java. Rispetto a XACML la sintassi di FACPL è molto più semplice e concisa, quindi permette di formalizzare in modo facile e rapido politiche di *access control*. Tuttavia, FACPL non gode di caratteristiche per eseguire richieste ed ottenere risposte valutando anche il comportamento passato, quindi l'obiettivo di questa tesi è stato quello di estenderlo in modo da implementare nuove e fondamentali funzionalità che permettono di sfruttare caratteristiche tipiche di *Usage Control*.

La tesi, dopo questa breve introduzione, è organizzata in questo modo:

- Nel Capitolo 2 vengono presentati in maggior dettaglio tutti i modelli di *Access Control* ed inoltre viene dedicata una sezione a *Usage Control* dove vengono anche introdotti due esempi che verranno portati avanti durante gli altri capitoli.
- Nel Capitolo 3 è descritto FACPL e vengono riportati alcuni esempi che mostrano le problematiche per cui non è possibile farne un uso a livello di *Usage Control*.
- Nel Capitolo 4 viene trattata l'estensione di FACPL ad un livello sintattico e semantico, spiegando quali nuove componenti sono state introdotte ed analizzandone il loro significato ed utilizzo attraverso dei casi di studio.
- Nel Capitolo 4 sono trattati gli argomenti visti in quello precedente ma dal punto di vista dell'estensione della libreria Java.
- Nel Capitolo 6 viene riassunto tutto il lavoro svolto e gli sviluppi futuri.
- In Appendice A viene proposto il codice completo.

ACCESS CONTROL E USAGE CONTROL

I sistemi informatici moderni sono capaci di condividere dati e risorse computazionali, ed impedire accessi non autorizzati è diventata una priorità inderogabile. I motivi che portano a questa decisione possono essere legati alla privacy o alla consistenza dei dati durante una computazione. Ad esempio, molte informazioni personali possono essere raccolte durante alcune attività quotidiane, dunque diventa necessario proteggere questi dati da malintenzionati. Per questo motivo esistono sistemi di Access Control, ovvero dei sistemi definiti da un insieme di condizioni che permettono di creare una prima linea difensiva contro accessi indesiderati.

Nella prima parte di questo capitolo vengono trattati in maggior dettaglio i vari modelli di controllo all'accesso proposti negli ultimi decenni, infine viene analizzato anche un nuovo modello chiamato *Usage Control*.

2.1 ACCESS CONTROL

Negli anni sono stati proposti diversi approcci per cercare di definire un modello efficiente e scalabile. Andremo ora ad eseguire una classificazione dei modelli di Access Control, seguendo la catalogazione del NIST [1].

- Access Control List è il primo di questi modelli ed è stato proposto intorno al 1970 spinto dall'avvento dei primi sistemi multi utente.
- Role Based Access Control è nato successivamente ad ACL e ne modifica alcuni aspetti in modo da rimuovere molte delle limitazioni di quest'ultimo.
- Attribute Based Access Control è nato dopo RBAC e fornisce un paradigma dinamico che aiuta a

- Policy Based Access Control è molto simile ad ABAC ma migliora e standardizza quest ultimo modello.

Access Control Lists (ACLs)

ACL è il primo modello di controlli agli accessi, è stato introdotto intorno agli anni 70 grazie all'avvento dei sistemi multi utente allo scopo di limitare l'accesso a file e dati condivisi, infatti i primi sistemi ad utilizzare questo modello sono stati sistemi di tipo UNIX. Con la comparsa della multiutenza per sistemi ad uso personale lo standard ACL è stato implementato in molte più ambienti come sistemi UNIX-Like e Windows.

Il concetto dietro ACL è uno dei più semplici, in quanto ogni risorsa del sistema che deve essere controllata ha una sua lista, che ad ogni soggetto associa le azioni che può effettuare sulla risorsa, ed il sistema operativo quando viene fatta richiesta decide in base alla lista se dare il permesso o meno.

Per esempio in Figura 1, si può vedere come *test_folder* sia la risorsa da controllare, *federicoschipani*, *staff* e *everyone* siano i soggetti e le azioni associate sono, in questo caso, *Read & Write* al primo soggetto e *Read only* agli altri due.

La semplicità di questo modello non richiede grandi infrastrutture sottostanti, la sua implementazione dal punto di vista applicativo risulta abbastanza semplice attraverso l'uso di linguaggi ad alto livello come Python o Java, poiché le strutture che servono per implementare questo standard sono già definite. Nonostante negli anni sono stati sviluppati modelli più complessi, come ABAC, PBAC e RBAC, il sistema descritto in questa sezione viene comunque usato nei sistemi operativi recenti. Come si può vedere in Figura 1 OS X sfrutta questo standard per la gestione dei permessi sul filesystem.

Un aspetto negativo si manifesta quando si trattano grandi quantità di risorse. Ogni volta che viene richiesto l'accesso ad una risorsa da parte di un entità, utente o applicazione che sia, è necessario verificare nella lista associata, il che lo rende abbastanza oneroso dal punto di vista computazionale.

Un altro lato negativo emerge quando bisogna effettuare modifiche ai permessi di una determinata risorsa, in quanto è necessario andare ad operare sulla lista di quest'ultima, il che rende questo compito incline ad errori ed oneroso dal punto di vista del tempo.

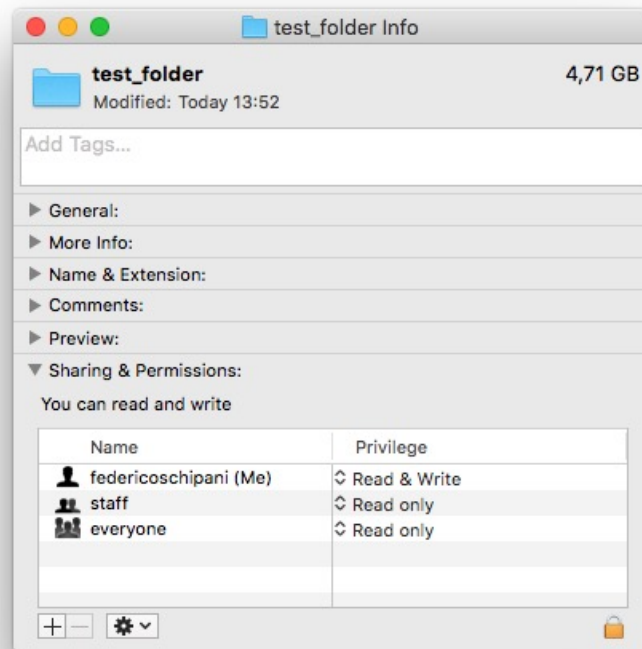


Figura 1.: ACL in OS X

Role-based Access Control (RBAC)

RBAC è l'evoluzione di ACL, in quanto tende a correggerne alcuni difetti come la limitata scalabilità.

A differenza di ACL è presente il concetto il ruolo del richiedente, ovvero un titolo che definisce un livello di autorità, che raggrupperà diversi utenti in una categoria. RBAC attraverso questa nuova caratteristica riesce a porre rimedio ai difetti di ACL in quanto questo tipo di gestione offre il vantaggio di facilitare l'assegnazione dei permessi, poiché per ogni risorsa non si devono più gestire tutti i singoli utenti, ma basta gestire i permessi associati a queste nuove categorie.

Un utente può anche far parte di più gruppi, per esempio un contabile di un'azienda può far parte del gruppo *impiegati* e *contabili* in modo da permettergli l'accesso sia ai documenti riservati ai soli impiegati che quelli riservati ai soli contabili. Come si può vedere in Figura 2 il concetto di gruppo è implementato nei sistemi operativi moderni, in particolare in OS X, Windows e sistemi UNIX-Like.

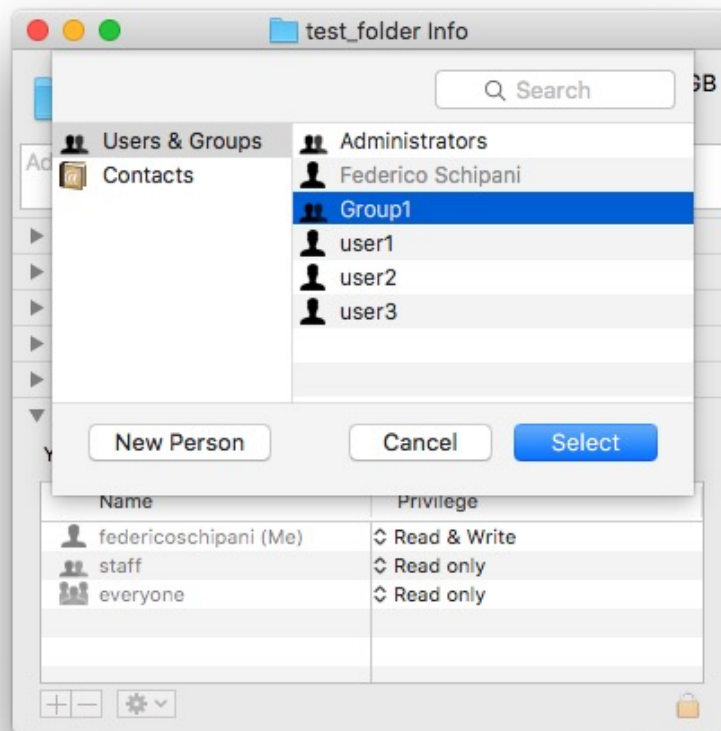


Figura 2.: Gruppo in OS X

RBAC però ha i suoi difetti, uno dei più evidenti è l'impossibilità di gestire le autorizzazioni a livello di singola persona, ed è quindi necessario creare diversi gruppi o trovare altri escamotage¹ per autorizzare, o vietare, singoli utenti appartenenti a determinati gruppi.

Attribute-based Access Control (ABAC)

ABAC è un modello di controllo all'accesso nel quale le decisioni sono prese in base ad un insieme di attributi, associazioni con il richiedente, ambiente e risorsa stessa. In questa nuova architettura è presente un nuovo componente chiamato Policy Decision Point (PDP) il quale si occuperà

¹ Gioco di destrezza con cui si sottrae qualche cosa all'attenzione degli interessati o dei presenti, gioco di bussolotti; in senso fig., inganno elegante o ingegnoso, gioco di abilità politica e diplomatica, o in genere sotterfugio per aggirare un ostacolo

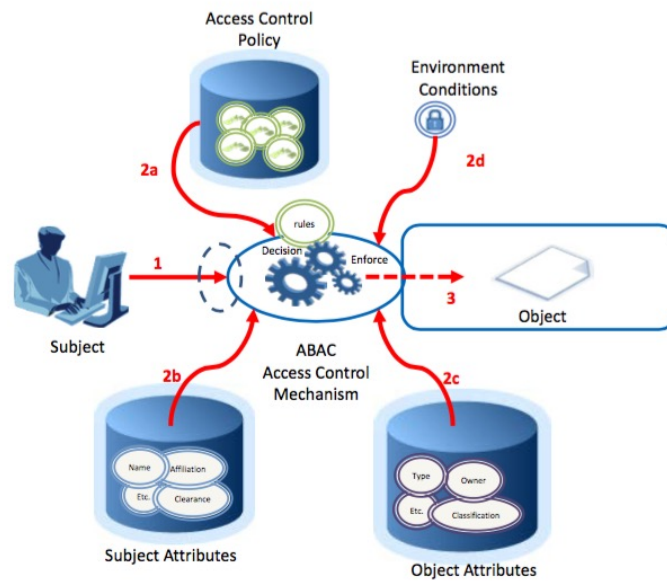


Figura 3.: Scenario ABAC base

della valutazione delle richieste prima di fornire una decisione finale. Ogni attributo è un campo distinto dagli altri che il PDP compara con un insieme di valori per determinare o meno l'accesso alla risorsa. In Figura 3 viene mostrato il funzionamento di ABAC. Di particolare rilevanza è il secondo step, che porta alla raccolta di tutte le informazioni per produrre una decisione finale. Inizialmente il sistema richiede al Access Control Policy (ACS) le policy, successivamente effettua la raccolta degli attributi dalle varie fonti. Questi attributi possono provenire da disparate fonti ed essere di svariati tipi. Per esempio nella valutazione di una richiesta possono essere considerati attributi come la data di assunzione di un dipendente ed il suo grado all'interno dell'azienda.

Un vantaggio di ABAC è che non c'è la necessità che il richiedente conosca in anticipo la risorsa o il sistema a cui dovrà accedere. Finché gli attributi che il richiedente fornisce coincidono con i requisiti dettati dalle policy l'accesso sarà garantito. ABAC perciò è utilizzato in situazioni in cui i proprietari delle risorse vogliono far accedere utenti che non conoscono direttamente a patto che però rispettino i criteri preposti, il che rende il tutto molto più dinamico rispetto ad ACL e RBAC.

Diversamente da ACL e RBAC questo tipo di controllo agli accessi non è implementato nei sistemi operativi, ma è largamente usato a livello applicativo. Spesso si usano applicazioni intermedie per mediare gli accessi da parte degli utenti a specifiche risorse. Implementazioni semplici di questo

modello non richiedono grandi *database* o altre infrastrutture, tuttavia in ambienti dove non basta una semplice applicazione c'è necessità di grandi banche di dati.

Una limitazione di ABAC è che in grandi ambienti, con tante risorse, individui e applicazioni ci saranno molte regole, ed organizzarle in maniera efficiente diventa un compito oneroso.

Policy-based Access Control (PBAC)

PBAC è stato sviluppato per far fronte alle problematiche di organizzazione delle regole di ABAC, infatti è una sua naturale evoluzione e tende ad uniformare ed armonizzare il sistema di controllo accessi. Questo modello cerca di aiutare le imprese a indirizzarsi verso la necessità di implementare un sistema di controllo agli accessi basato su policy.

PBAC combina attributi dalle risorse, dall'ambiente e dal richiedente con informazioni su determinate circostanze sotto le quali la richiesta è stata effettuata ed inoltre si serve di ruoli per determinare quando l'accesso è garantito.

Nei sistemi ABAC gli attributi richiesti per avere accesso ad una particolare risorsa sono determinati a livello locale e possono variare da organizzazione ad organizzazione. Per esempio, un'unità organizzativa può determinare che l'accesso ad un archivio di documenti sensibili è semplicemente soggetto a richiesta di credenziali e ruolo particolare. Un'altra unità invece, oltre a richiedere credenziali e ruolo, richiede anche un certificato. Se un documento viene trasferito dal secondo al primo archivio perde la protezione fornita da quest'ultimo e sarà soggetto solo alla richiesta di credenziali e ruolo. Con PBAC invece si ha un solo punto dove vengono gestite le policy, e queste policy verranno eseguite ad ogni tentativo di accedere alla risorsa. PBAC quindi è un sistema molto più complicato di ABAC e perciò richiede il dislocamento di infrastrutture molto più onerose dal punto di vista economico che includono *database*, *directory service* e altri applicativi di mediazione e gestione. PBAC non richiede solo un'applicazione per gestire la valutazione delle policy, ma anche un sistema per la scrittura di queste ultime in modo che non risultino ambigue. Uno standard basato su eXtensible Markup Language (XML), e che si chiama XACML, è sviluppato in modo tale da creare policy facilmente leggibili da una macchina.

Sfortunatamente però, queste policy non sono facili da scrivere e l'uso di XACML non necessariamente rende facile il processo di creazione, specifica e valutazione corretta di una policy.

Ci vorrebbe anche un modo per assicurarsi che tutti gli utenti di un sistema utilizzino lo stesso insieme di attributi, piuttosto arduo da realizzare. Gli attributi dovrebbero essere forniti da un'entità chiamata *Authoritative Attribute Source* (AAS) che, oltre a fare da sorgente per gli attributi, deve anche occuparsi della loro consistenza. In più bisogna instaurare un meccanismo per verificare che questi attributi provengano realmente dall'AAS. Come detto prima può sembrare facile fare una cosa del genere, ma bisogna considerare il caso in cui più aziende lavorano insieme e devono implementare un sistema di controllo degli accessi in comune. Un problema si può verificare quando un'azienda valuta la gestione dell'AAS tramite una particolare *repository*, ma un'altra azienda non è d'accordo a questo tipo di soluzione

2.2 USAGE CONTROL

Oggi sono presenti differenti tipi di sistemi diversi che richiedono un modello più flessibile e continuativo per gestire la sicurezza. Questa sezione parlerà di un nuovo sistema, chiamato *Usage Control* [2].

Usage Control si propone come un nuovo e promettente approccio per l'*Access Control*. In particolare verrà trattato il modello, inizialmente proposto da Sandhu e Park[2], chiamato $UCON_{ABC}$.

$UCON_{ABC}$ utilizza un approccio diverso rispetto a *Access Control* in quanto, rispetto a quest'ultimo, si riesce ad avere una continuità delle decisioni sull'accesso. Ciò vuol dire che le decisioni non vengono più prese decisioni solo a priori, ma anche durante l'accesso. Quindi, se durante l'utilizzo, qualche attributo di stato cambia e la *policy* non è più soddisfatta viene revocato l'accesso. Di conseguenza è richiesto un componente che modella lo stato del sistema, in modo tale da effettuare valutazioni in base a quelle effettuate in precedenza.

Il vantaggio di *Usage Control* è la sua capacità di adattarsi a vari casi di utilizzo, riuscendo così a includere e migliorare sistemi come ACL, RBAC, ABAC e PBAC descritti in 2.1. Il passaggio da *Access Control* a *Usage Control* è importante soprattutto quando si va a considerare ambienti legati alla rete, come possono essere il web o il cloud.

Il processo decisionale in *Usage Control* è diviso in due fasi [3].

- La prima fase è una fase di *pre decision* che fondamentalmente è la classica decisione presa in *Access Control*, questa decisione viene presa al momento in cui è effettuata la prima richiesta per produrre la decisione di accesso.

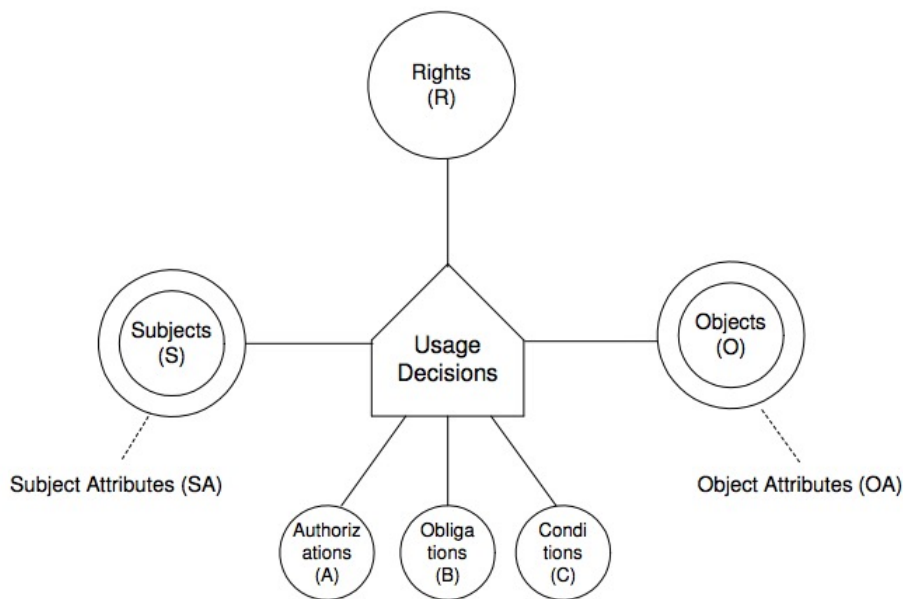


Figura 4.: Insieme dei componenti di $UCON_{ABC}$

- La seconda fase è chiamata *ongoing decision*, ed è un processo che implementa il concetto di continuità in quanto le decisioni vengono prese durante l'accesso.

I componenti necessari a questo tipo di processo decisionale sono dei predicati, che possono essere di tre tipi, *authorizations*, *conditions* oppure *rights*, delle azioni chiamate *obligations* che devono essere eseguite durante l'accesso ed infine uno stato. Come questi componenti contribuiscono a prendere una decisione viene mostrato in Figura 4.

2.2.1 Caso di studio 1: Gestione lettura e scrittura di file

Dentro ad un sistema ci sono vari file, ai quali per questione di consistenza, bisogna limitare l'accesso. La regola è: "per un determinato file un massimo di due persone possono accedere in lettura oppure solo una persona può accedere in scrittura". In Figura 5 viene mostrato un diagramma di flusso che sintetizza, e permette di capire meglio, la regola di accesso. Quando arriva la richiesta viene verificata la presenza nel database del richiedente e del file richiesto, se entrambe danno esito positivo si passa all'analisi dei requisiti per soddisfare la richiesta.

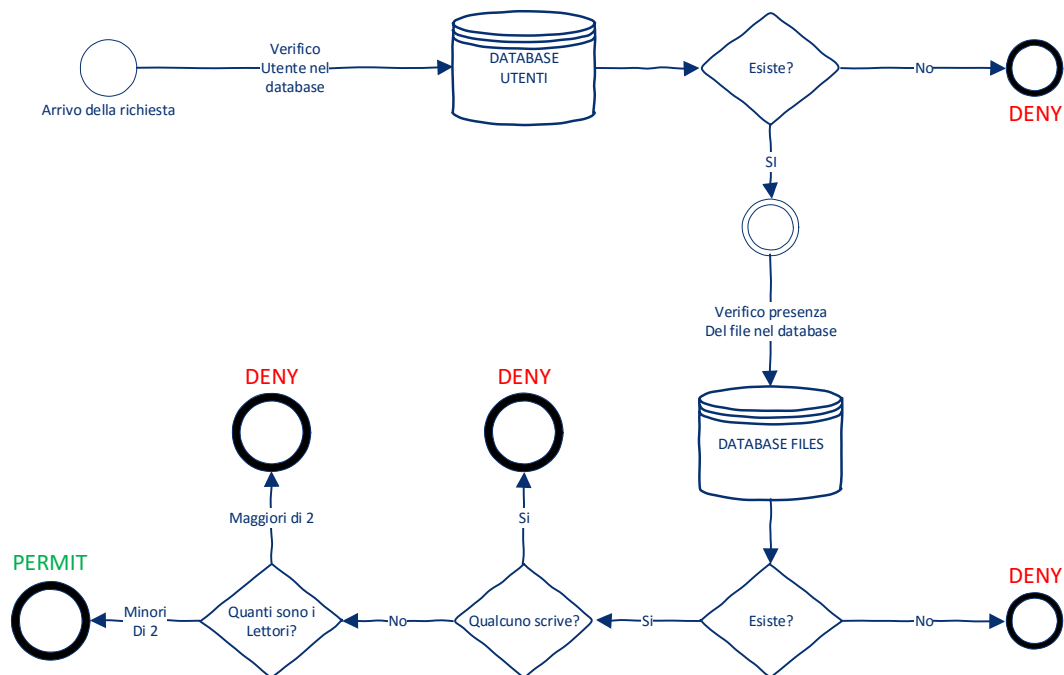


Figura 5.: Diagramma di flusso del primo esempio

In un primo momento nessuno sta visualizzando o scrivendo un determinato file, ed un utente generico chiederà l'accesso in lettura per questo file, ovviamente il responso sarà positivo in quanto non viola la regola preposta prima.

Dopo un po' di tempo, mentre il primo sta ancora leggendo, un altro utente chiede l'accesso in scrittura, che gli viene negato. In un istante di tempo successivo il primo utente sta continuando a leggere, ed anche il secondo utente vuole leggere. In questo caso viene dato responso positivo.

Infine, entrambi gli utenti smettono di leggere, ma uno di loro vuole apportare una modifica, allora richiede l'accesso in scrittura, che questa volta gli viene consentito poiché nessuno sta leggendo.

2.2.2 Caso di studio 2: Noleggio e acquisto di contenuti

Un altro utilizzo possibile di *Usage Control* riguarda l'analisi del comportamento passato. Un'azienda fornisce ai propri clienti la possibilità di effettuare noleggi o acquisti di contenuti multimediali (musica, video,

film, serie tv e via scorrendo).

In caso il contenuto fosse stato acquistato, l'acquirente potrà ottenere l'accesso infinite volte per infinito tempo. Nel caso di noleggio invece saranno presenti delle condizioni, come per esempio il massimo numero di fruizioni del contenuto o una data di scadenza che, una volta oltrepassata, impedirà l'ulteriore visione del contenuto noleggiato in precedenza.

Come nell'esempio precedente viene proposto un diagramma di flusso, proposto Figura 6, che permette di capire meglio il funzionamento questo sistema di *Usage Control*. Innanzitutto viene verificata la presenza nei due relativi database dell'utente e del file richiesto, successivamente viene analizzata la richiesta, che può essere di tre tipi.

- Visione: nel caso la richiesta fosse di visione viene verificato se realmente l'utente ha diritto ad avere accesso a quella risorsa, e di conseguenza viene presa una decisione.
- Acquisto: nel caso la richiesta fosse di acquisto verrà accreditato l'acquisto all'utente che ha effettuato la richiesta.
- Noleggio: per questa forma ci sono due diverse tipologie, il noleggio a tempo e il noleggio a numero di visualizzazioni. Nel primo caso all'utente sarà concesso di vedere il file per un determinato periodo di tempo, mentre nel secondo il richiedente potrà visionare il file per un numero limitato di volte.

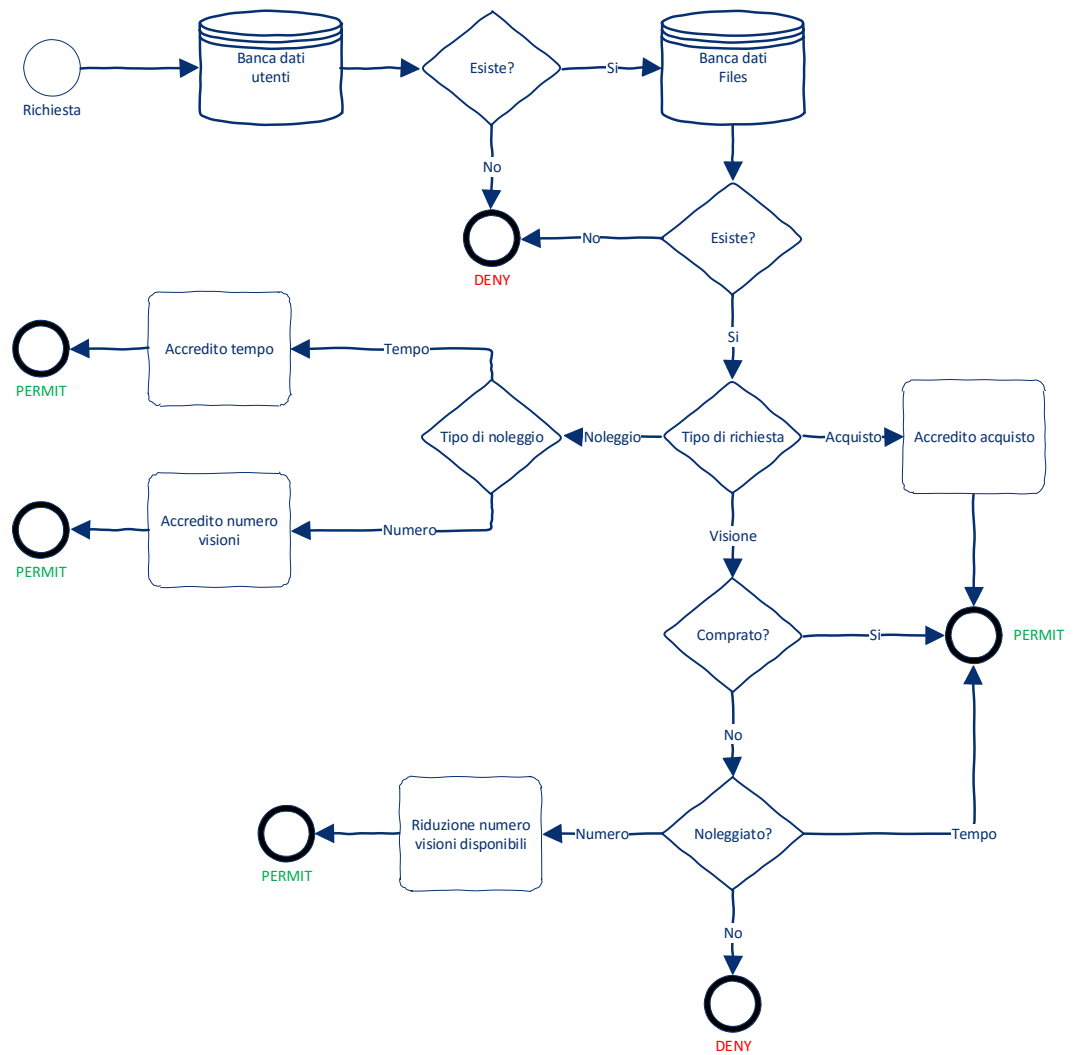


Figura 6.: Diagramma di flusso del secondo esempio

FORMAL ACCESS CONTROL POLICY LANGUAGE

Negli anni molti linguaggi sono stati proposti per definire policy di access control. Uno di questi è stato rilasciato nel 2003 da parte di OASIS ed il suo nome è *eXtensible Access Control Markup Language* (XACML). Questo linguaggio ha una sintassi basata su XML e fornisce caratteristiche avanzate per l'*Access Control*. Il problema fondamentale di XACML è che non ha una sintassi facile da leggere e da scrivere.

L'obiettivo di *Formal Access Control Policy Language* (FACPL) è definire una sintassi alternativa per XACML in modo da renderlo più agevole da usare. FACPL quindi è parzialmente ispirato a XACML, ma oltre ad introdurre una nuova sintassi ridefinisce alcuni aspetti aggiungendo nuove caratteristiche. Il suo scopo però non è sostituire XACML, ma fornire un linguaggio compatto ed espressivo per facilitare le tecniche di analisi attraverso tool specifici.

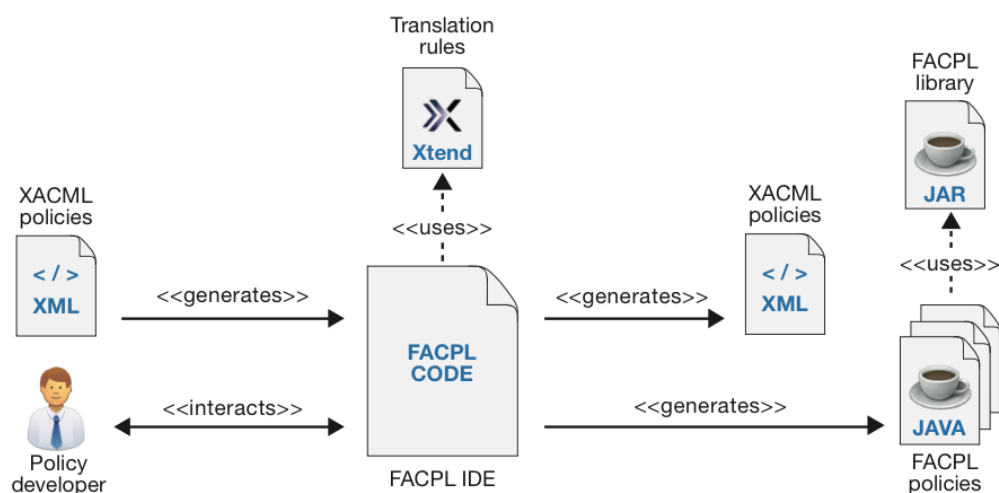


Figura 7.: ToolChain di FACPL

3.1 IL PROCESSO DI VALUTAZIONE DI FACPL

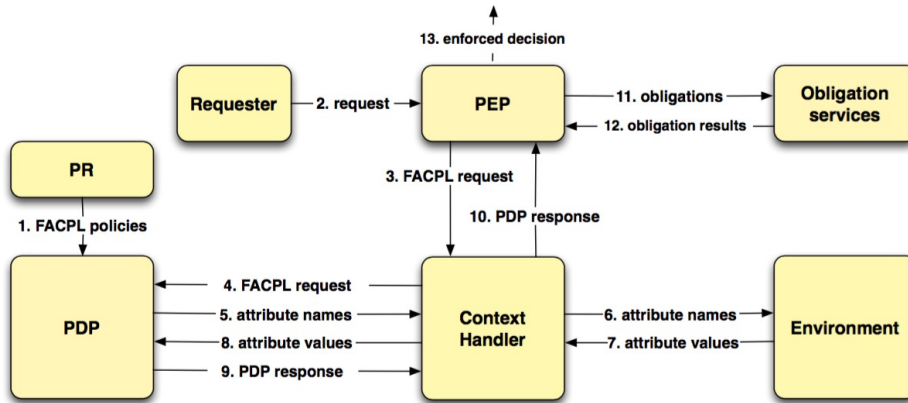


Figura 8.: Il processo di valutazione di FACPL

In figura 8 è mostrato il processo di valutazione delle policy definite in FACPL. I componenti principali sono tre:

- Policy Repository (PR)
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)

Le policy sono memorizzate nel PR, il quale le rende disponibili al PDP che deciderà, successivamente, se garantire l'accesso o meno (Primo step). Nello step 2, quando il PEP riceve una richiesta, le credenziali di quest'ultima vengono codificate in una sequenza di attributi (ogni attributo è una coppia stringa valore) che, nello step 3, andranno a loro volta a formare una *FACPL Request*. Al quarto step il *context handler* aggiungerà attributi di ambiente (per esempio l'ora di ricezione della richiesta) e manderà la richiesta al PDP. A questo punto il PDP, tra il quinto e l'ottavo step, valuterà la richiesta e fornirà un risultato, il quale può eventualmente contenere delle *obligations*. La decisione del PDP può essere di quattro tipi, permit, deny, not-applicable o indeterminate. Il significato delle prime due decisioni è facilmente intuibile, mentre per le ultime due vuol dire che c'è stato un errore durante la valutazione. Gli errori possono essere di diverso tipo, e vengono gestiti attraverso algoritmi che combinano le decisioni delle varie policy per ottenere un risultato finale. Le *obligations* sono azioni, eseguite dal PEP, correlate al

sistema di controllo degli accessi. Queste azioni possono essere di svariati tipi, come per esempio generare un file di log, o mandare una mail. Allo step 13, sulla base del risultato delle *obligations*, il PEP esegue un processo chiamato *Enforcement* il quale restituirà un'altra decisione. Quest'ultima decisione corrisponde alla decisione finale del sistema e può differire da quella del PDP.

3.2 LA SINTASSI DI FACPL

La sintassi di FACPL è definita nella tabella 1. La sintassi è fornita come una grammatica di tipo EBNF, dove il simbolo ? corrisponde ad un elemento opzionale, il simbolo * corrisponde ad una sequenza con un numero arbitrario di elementi (anche 0), ed il simbolo + corrisponde ad una sequenza non vuota con un numero arbitrario di elementi.

Al livello più alto c'è il *Policy Authorisation System (PAS)*, il quale definisce le specifiche del PEP e del PDP. Il PEP è definito semplicemente come un *enforcing algorithm* che sarà applicato per decidere su quali decisioni verrà eseguito il processo di *enforcement*.

Il PDP invece è definito come una sequenza (non vuota) di *Policy*, ed un algoritmo di combining che combinerà i risultati di queste *policy* per ottenere un unico risultato finale.

Una *policy* può essere una semplice *rule* o una *policy set*, quest'ultima avrà al suo interno altre *policy set* o *rule*, ed in questo modo viene formata una gerarchia di *policy*.

Un *policy set* individua un target, che è una espressione che indica il set di richieste di accesso alla quale si applica la *policy*, una lista di *obligations*, che definiscono azioni obbligatorie o opzionali che devono essere eseguite nel processo di *enforcement*, una sequenza di altre *policy*, ed un algoritmo per combinarle.

Una *rule* includerà un *effect*, che sarà permit o deny quando la regola è valutata correttamente, un target ed una lista di *obligations*.

Le *Expressions* sono formate da *attribute names* e valori (per esempio boolean, double, strings, date).

Tabella 1.: Sintassi di FACPL

Policy Authorisation Systems	$PAS ::= (pep : EnfAlg \ pdp : PDP)$
Enforcement algorithms	$EnfAlg ::= base \mid deny\text{-}biased \mid permit\text{-}biased$
Policy Decision Points	$PDP ::= \{Alg \ policies : Policy^+\}$
Combining algorithms	$Alg ::= p\text{-}over_\delta \mid d\text{-}over_\delta \mid d\text{-}unless\text{-}p_\delta \mid p\text{-}unless\text{-}d_\delta$ $\mid first\text{-}app_\delta \mid one\text{-}app_\delta \mid weak\text{-}con_\delta \mid strong\text{-}con_\delta$
fulfilment strategies	$\delta ::= greedy \mid all$
Policies	$Policy ::= (Effect \ target : Expr \ obl : Obligation^*)$ $\mid \{Alg \ target : Expr$ $\quad policies : Policy^+ \ obl : Obligation^*\}$
Effects	$Effect ::= permit \mid deny$
Obligations	$Obligation ::= [Effect \ ObType \ PepAction(Expr^*)]$
Obligation Types	$ObType ::= M \mid O$
Expressions	$Expr ::= Name \mid Value$ $\mid and(Expr, Expr) \mid or(Expr, Expr) \mid not(Expr)$ $\mid equal(Expr, Expr) \mid in(Expr, Expr)$ $\mid greater\text{-}than(Expr, Expr) \mid add(Expr, Expr)$ $\mid subtract(Expr, Expr) \mid divide(Expr, Expr)$ $\mid multiply(Expr, Expr)$
Attribute Names	$Name ::= Identifier / Identifier$
Literal Values	$Value ::= true \mid false \mid Double \mid String \mid Date$
Requests	$Request ::= (Name, Value)^+$

Un *Attribute Name* indica il valore di un attributo che può essere contenuto nella richiesta o nel contesto. FACPL usa per gli *Attribute Name* una forma del tipo *Identifier / Identifier*, dove il primo *Identifier* indica la categoria, ed il secondo il nome dell'attributo. Per esempio *Action / ID* rappresenta il valore di un attributo ID di categoria Action.

I *Combining Algorithm* implementano diverse strategie che servono per

Tabella 2.: Sintassi ausiliaria per le risposte

PDP Responses	$PDPResponse ::= \langle Decision \ FObligation^* \rangle$
Decisions	$Decision ::= \text{permit} \mid \text{deny} \mid \text{not-app} \mid \text{indet}$
Fulfilled obligations	$FObligation ::= [ObType \ PepAction(Value^*)]$

risolvere conflitti tra le varie decisioni, restituendo alla fine un'unica decisione finale.

Una *obligation* ha al suo interno un effect, un tipo, ed una azione eseguita dal PEP con la relativa *Expression*.

Una *request* consiste di una sequenza di attributi organizzati in categorie.

La risposta ad una valutazione di una richiesta FACPL è scritta usando la sintassi riportata in tabella 2. La valutazione in due step, descritta precedentemente in sezione 3.1, produce due tipi di risultati. Il primo è la risposta del PDP, il secondo è una decisione, ovvero una risposta del PEP. La decisione del PDP, nel caso in cui ritorni permit o deny, viene associata ad una lista, anche vuota, di *fulfilled obligation*.

Una *fulfilled obligation* è una semplice coppia formata da un tipo (M o O) ed una azione i quali argomenti sono ottenuti dalla valutazione del PDP.

3.3 LA SEMANTICA DI FACPL

Molteplici sono le componenti di FACPL, e la semantica ora verrà informalmente analizzata [6]. Prima verrà presentato il processo che porterà ad una risposta del PDP, successivamente il processo di *enforcement* del PEP.

Quando il PDP riceve una richiesta, per prima cosa la valuta sulle basi delle *policy* disponibili, successivamente determinerà un risultato combinando le decisioni ritornate da queste *policy* attraverso degli algoritmi di combining.

La valutazione della *policy* rispetto alla richiesta comincia verificando l'applicabilità alla richiesta, che è fatta valutando un'espressione definita *target*.

Si possono valutare due casi distinti:

- Supponiamo che l'applicabilità dia esito positivo, nel caso ci sia una *rule* sarà ritornato il valore risultante dalla valutazione di quest'ultima, mentre se c'è un *policy set* il risultato è ottenuto valutando le *policy* contenute all'interno, e combinando i loro valori con un algoritmo specificato in fase di creazione del PDP. Successivamente a queste valutazioni verrà effettuato il *fulfilment* delle *obligation* contenute all'interno delle *policy*.
- Supponiamo ora che l'applicabilità non dia esito positivo, ovvero la valutazione del *target* restituisca false. In questo caso il risultato della *policy* sarà not-app. Mentre se il *target* restituisce un valore non booleano o ritorna un errore il risultato della *policy* sarà indet.

Valutare le espressioni corrisponde ad applicare degli operatori e risolvere i nomi degli attributi che contengono, e di conseguenza ricavarne un valore.

Se non è possibile trovare un attributo, magari perché non esiste, viene ritornato un valore speciale, chiamato BOTTOM. Questo valore può essere usato per implementare diverse strategie per gestire l'assenza di attributi. FACPL gestisce questo valore come una specie di false, quindi permette la mancanza di attributi senza la generazione di errori.

La valutazione di un'espressione tiene conto anche dei tipi degli argomenti. Se l'argomento è del tipo aspettato l'operatore viene applicato correttamente, sennò, se un argomento è BOTTOM e nessun'altro è error viene ritornato BOTTOM, mentre se almeno uno di essi è error, viene ritornato error.

Con l'operatore and o or il trattamento sarà leggermente diverso, in quanto BOTTOM viene ritornato solo se un argomento è tale e nessun'altro è false o error, mentre in caso contrario viene ritornato error.

La valutazione di una *policy* termina con il *fulfillment* di tutte le *obligations* le quali hanno il valore di applicabilità coincidente con quello ritornato dalla valutazione della *policy*. Quest'operazione consiste nel valutare

tutte le espressioni presenti al interno delle *obligations* coinvolte nel processo. Se ci sarà un errore nel processo di *fulfillment* allora il risultato della *policy* sarà *indet*, altrimenti il risultato del *fulfillment* sarà uguale a quello della valutazione del PDP.

Gli algoritmi di combining, come detto prima hanno lo scopo di combinare le decisioni risultanti dalla valutazione delle richieste in accordo con le *policy*. Un'altra funzione che hanno è ritornare le *obligations* corrette nel caso in cui la valutazione finale risulti *permit* o *deny*. Questa famiglia di algoritmi ha una strategia δ che viene usata per restituire le *obligation*, e può essere di due tipi. Il primo tipo è la strategia *all* (tutto), ovvero richiede la valutazione di tutte le *policy* e ritorna le *fulfilled obligation* pertinenti a tutte le decisioni.

Il secondo tipo è la strategia *greedy* (golosa), la quale prescrive che l'esecuzione si debba arrestare appena è ottenuta una decisione che non può cambiare a causa della valutazione di susseguenti *policy* nella sequenza di input.

Come ultimo step il risultato del PDP viene mandato al PEP per l'enforcement. Il PEP per effettuare questo processo deve eseguire l'azione all'interno di ogni *fulfilled obligation* e decidere come comportarsi per le decisioni di tipo *not-app* e *indet*.

Per fare questo processo usa delle strategie. In particolare, l'algoritmo *deny-biased* (rispettivamente, *permit-based*) effettua l'enforcement dei *permit* (rispettivamente *deny*) solo quando tutte le corrispondenti *obligations* sono correttamente eseguite, mentre effettua l'enforcement dei *deny* (rispettivamente *permit*) in tutti gli altri casi. Invece, l'algoritmo di base lascia tutte le decisioni non cambiate ma, in caso di decisioni *permit* e *deny*, effettua l'enforcement di *indet* se ci sarà un errore durante l'esecuzione delle *obligations*. Questo evidenzia che le *obligations* non solo influenzano il processo di autorizzazione, ma anche l'enforcement. Gli errori causati dalle *obligations* con tipo *O* vengono ignorati.

3.4 ESEMPIO DI POLITICA CON FACPL

In questa sezione verrà analizzata una semplice politica scritta in FACPL con delle eventuali richieste.

Codice 3.1: Esempio di politica in FACPL

```

PolicySet fileRule { permit-overrides
  target:
    equal("458", resource/resource-id)
  policies:
    Rule writeRule ( permit target:
      equal ("WRITE" , subject/action )
      && equal ("ADMINISTRATOR", subject/role)
    )
    Rule writePeronio ( permit target:
      equal("PERONIO", subject/id)
    )
    Rule denyRule ( deny target:
      equal("GUEST", subject/role) )
  obl:
    [ deny M action2 (subject / id )]
    [ permit M action1 (subject / id)]
}

```

Con questo codice si vuole ottenere lo scopo di regolare l'accesso ad una risorsa chiamata 458. In questo caso gli utenti che hanno ruolo *GUEST* non possono accedere, mentre gli *ADMINISTRATOR* sì, fatta eccezione per l'utente Peronio, che qualunque ruolo abbia può accedere. Le richieste effettuate al sistema vengono mostrate in Codice 3.2, e sono tre. La prima proviene dall'utente Gianfabrizio che fa parte degli *ADMINISTRATOR*, la seconda e la terza rispettivamente dall'utente Gianpietro e Peronio che fanno entrambi parte dei *GUEST*.

Codice 3.2: Richieste per Codice 3.1

```

Request:{ Request1
  (subject/action , "WRITE")
  (subject/role , "ADMINISTRATOR")
  (resource/resource-id , "458")
  (subject/id, "GianFabrizio")
}
Request:{ Request2
  (subject/action , "WRITE")
  (subject/role , "GUEST")
  (resource/resource-id , "458")
  (subject/id, "GianPietro")
}
Request:{ Request3

```



```
(subject/action , "WRITE")
(subject/role , "GUEST")
(resource/resource-id , "458")
(subject/id, "PERONIO")
}
```

L'output prodotto dalle seguenti richieste è il seguente:

```
Request: Request1
  Authorization Decision: PERMIT
  Obligations: PERMIT M action1([GianFabrizio])
Request: Request2
  Authorization Decision: DENY
  Obligations: DENY M action2([GianPietro])
Request: Request3
  Authorization Decision: PERMIT
  Obligations: PERMIT M action1([PERONIO])
```

Ovviamente alla prima richiesta il risultato è permit, in quanto l'utente è un amministratore. Alla seconda richiesta il risultato è deny poiché l'utente è un ospite, mentre alla terza, nonostante l'utente faccia parte dello stesso gruppo del secondo riesce ad ottenere risultato permit per via della regola che considera il suo nome.

FACPL, come mostrato dall'esempio, permette di fare richieste ed ottenere delle risposte, ma queste richieste sono totalmente indipendenti l'una dall'altra, quindi l'ordine di esecuzione non avrebbe influenzato in alcun modo il risultato finale. In sezione 2.2 sono stati introdotti due esempi i quali non possono, per ora, essere implementati in FACPL poiché manca quest'aspetto che crea dipendenza tra le richieste. Per creare questa dipendenza tra richieste è necessario che il sistema si ricordi in qualche modo quello che è successo prima, perciò si inizia a parlare di un nuovo concetto che può essere assimilabile ad uno stato. Lo scopo del Capitolo 4 e 5 è proprio permettere a FACPL questo tipo di valutazione.

IMPLEMENTARE USAGE CONTROL IN FACPL

FACPL, fino alla versione descritta nel capitolo 3, non aveva la possibilità di essere sfruttato per *Usage Control*.

Grazie a delle nuove strutture implementate insieme al mio collega Filippo Mameli, adesso è possibile usare FACPL per *Usage Control*, introducendo miglioramenti descritti in 2.2.

La nuova funzionalità consiste nel prendere decisioni tenendo conto delle richieste già effettuate. Introdurre questa nuova estensione ha richiesto del lavoro sulla libreria, in quanto è stato necessario aggiungere nuove componenti e di conseguenza modificare il processo di valutazione di una policy. Infine è stato necessario anche introdurre delle modifiche alla sintassi del linguaggio in modo da poterle sfruttare facilmente.

4.1 ESTENSIONE DEL PROCESSO DI VALUTAZIONE

Il processo di valutazione è stato esteso per via delle modifiche introdotte. Rispetto al processo di valutazione standard, descritto in sezione 3.1, sono state aggiunte componenti al grafico, rendendolo così adatto allo *Usage Control*, in particolare alla valutazione di richieste basate sul comportamento passato.

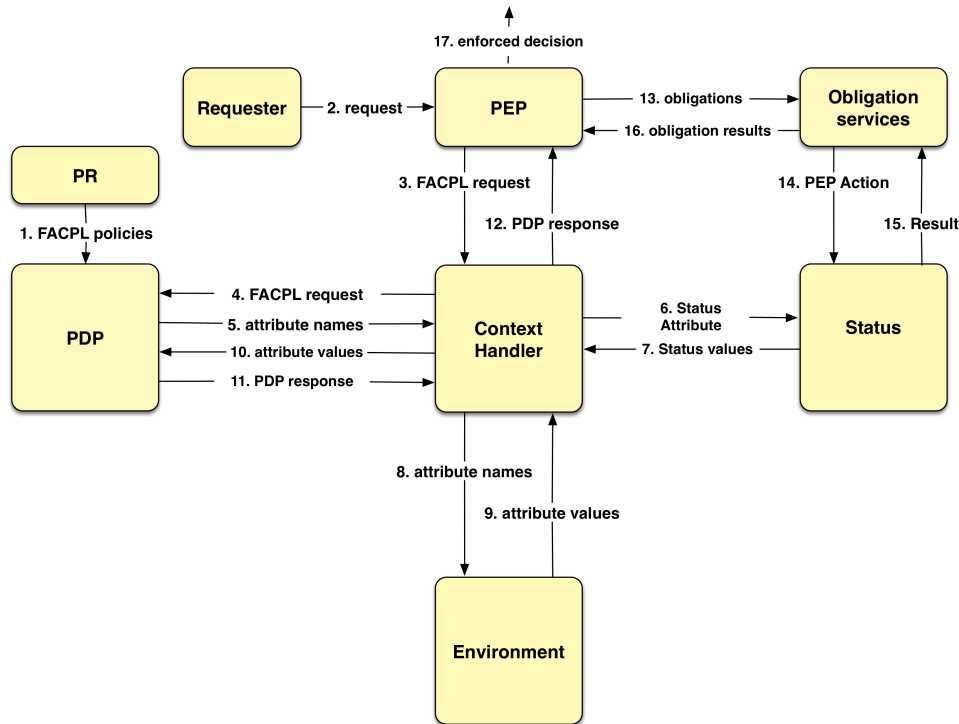


Figura 9.: Nuovo processo di valutazione in FACPL

Come si nota in figura 9 è stato aggiunto un componente alla struttura della valutazione. Questo componente è lo *Status* (Stato), ovvero un semplice contenitore di un nuovo tipo di attributi. I nuovi attributi vengono chiamati *Status Attribute*. Ovviamente quest'estensione non modifica il comportamento nel caso di assenza di stato, di conseguenza la valutazione rimane inalterata rispetto a quella descritta precedentemente, mentre viene modificata nel caso in cui lo stato sia presente in modo da gestire correttamente la presenza di esso.

Analizziamo quindi, a scopo esemplificativo, il secondo caso, ovvero quando lo stato è presente. Inizialmente viene definito il sistema, che ora ha quattro componenti principali:

- Policy Repository (PR)
- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)
- Status

Fino al quarto step il comportamento è analogo a quello precedente, mentre cambia negli step successivi.

Al quinto step il *PDP* non necessiterà solo dei normali attributi d'ambiente, ma necessiterà anche degli *Status Attribute* coinvolti nella richiesta effettuata. Il *Context Handler* quindi non andrà solo a fare la ricerca all'interno dell'environment, ma andrà a cercare anche gli *Status Attribute* all'interno dello *Status*.

A questo punto, quando il *PDP* avrà tutte le informazioni necessarie si potrà passare alla vera e propria valutazione della richiesta che avviene come sempre.

Nel caso in cui viene restituito permit o deny è necessario fare l'enforcement della risposta del *PDP*. Questo processo differisce dal precedente poiché ora sono state implementate nuove azioni sullo stato che devono essere eseguite dal *PEP* (Passo 13-16). Una volta effettuato l'enforcement viene restituita la decisione finale.

Prendendo il primo esempio citato in sezione 2.2 la valutazione procederebbe in questo modo. Bob richiederà la lettura di un determinato file. Quindi la richiesta conterrà tre attributi, uno che indica il nome dell'utente che effettua la richiesta, il secondo che contiene il nome del file a cui si effettuerà l'accesso, e il terzo che conterrà il nome dell'azione da effettuare. La policy invece sarà strutturata come "*Se il nome è Bob, il file è corretto e nessuno sta scrivendo o ci sono meno di due utenti che leggono, allora permetti, altrimenti nega*".

Il *PDP* però ha bisogno di più attributi per valutare la richiesta, in quanto necessita anche di attributi esterni alla policy che riguardano il numero di utenti che stanno accedendo al file richiesto, questi attributi sono gli *Status Attribute*. Per la loro gestione sarà necessario utilizzare la funzionalità che riguarda l'Usage Control, il *PDP* richiederà al *Context Handler* questi attributi, il quale andrà cercarli nello *Status*. Quest'ultimo li fornirà e verranno direttamente mandati al *PDP* per la valutazione della richiesta.

Se la richiesta avrà esito positivo, allora vuol dire che Bob avrà accesso al file, e quindi lo stato andrà aggiornato. La risposta del *PDP* a questo punto andrà al *PEP* per l'enforcement il quale avrà il compito di aggiornare lo stato. Sostanzialmente lo stato viene aggiornato semplicemente

incrementando l'attributo riguardante il numero di lettori di un'unità.

4.2 ESTENSIONE LINGUISTICA

Per implementare queste nuove funzionalità è stata modificata anche la grammatica di FACPL. Nella grammatica estesa sono state aggiunte nuove regole di produzione e simboli terminali che codificano le nuove funzionalità.

Come è facilmente osservabile dalla consultazione della tabella 3 le aggiunte rispetto alla tabella riporta in sezione 3.2 sono state diverse, vediamo adesso quali sono.

La prima modifica che risulta evidente è nel PAS, ovvero nella definizione del sistema. L'aggiunta è stata lo *Status*, ovvero un contenitore di attributi. Uno *Status* è della forma

$$(\text{status} : \text{Attribute}^+)^?$$

questo significa che se lo *Status* è presente sarà formato da uno o più *Attribute*.

Passiamo ora a descrivere *Attribute* che è della forma

$$(\text{Type Identifier}(= \text{Value})^?)$$

questo tipo particolare di attribute, che è lo *Status Attribute* descritto in precedenza, è formato innanzitutto da un *Type*, dopo il tipo è richiesta una generica stringa chiamata *Identifier*, che sarà un generico nome da dare all'attributo, infine viene richiesto un *Value*, ovvero un valore, che in questo caso è opzionale, all'atto pratico vuol dire che l'attributo di stato potrà essere inizializzato con un valore oppure potrà essere solamente definito, lasciando che il valore sia quello di default.

Type è il tipo che avrà l'attributo di stato, e potrà essere `int`, `boolean`, `date` o `float`.

La regola *PepAction* è stata modificata in modo tale che includesse nuove funzioni per operare matematicamente sugli attributi di stato. Queste nuove funzioni sono:

- *add(Attribute, int)*

- *add(Attribute, float)*
- *div(Attribute, int)*
- *div(Attribute, float)*
- *sub(Attribute, int)*
- *sub(Attribute, float)*
- *mul(Attribute, int)*
- *mul(Attribute, float)*
- *flag(Attribute, boolean)*
- *sumDate(Attribute, date)*
- *sumString(Attribute, string)*
- *setValue(Attribute, string)*
- *setDate(Attribute, date)*

Infine l'ultima regola di produzione modificata è stata quella riguardante *Attribute Names*, in questo caso è stata semplicemente aggiunto, a fianco di *Identifier/Identifier*, una nuova produzione *Status/Identifier*. Questa nuova produzione serve semplicemente per permettere il confronto tra attributi di stato attraverso le già esistenti *Expression*. La sintassi delle risposte è rimasta invariata. Vediamo ora un esempio di questa nuova sintassi, prenderemo spunto da un caso già trattato in precedenza nella sezione 4.1.

Codice 4.1: Esempio per la sintassi

```

Policy example < permit-overrides
  target: equal("Bob",name/id) && equal("read", action/id)
  rules:
    Rule access (
      permit target: less-than(status/counter, 2))
    obl:
      [ permit M add(counter, 1)]
>

PAS {
  Combined Decision : false ;
  Extended Indeterminate : false ;

```

```

Java Package : "example" ;
Requests To Evaluate : Request_example ;
pep:  deny- biased
pdp:  deny- unless- permit
status: [(int counter = 0)]
include example
}

```

In questo esempio (Codice 4.1) si può vedere come nel PAS è stato definito uno stato, con al suo interno uno solo attributo inizializzato con valore 0. Successivamente si può notare nella *Rule* che viene fatto un controllo sul valore di quest'attributo. Infine nella *Obligation* si può notare come viene aggiornato lo stato dell'attributo in base al risultato della valutazione della *Rule*.

4.3 SEMANTICA

Sostanzialmente la semantica di FACPL rimane molto simile a quella descritta in sezione 3.3, quindi verranno di seguito descritte in modo informale solo le novità introdotte.

La prima di queste riguarda la valutazione delle richieste dal PDP. Il PDP ora non si deve più basare solo su richieste totalmente scollegate l'una dall'altra, e quindi è stato introdotto il concetto di *Status*. Lo stato serve per l'appunto per memorizzare il comportamento passato del sistema, e lo fa introducendo una nuova serie di attributi chiamati *Status Attribute*.

Nel linguaggio questo nuovo tipo di attributi viene considerato al pari di normali attributi, quindi si ha la possibilità di effettuare tutte le operazioni di confronto tra di essi, ma in più si deve avere la possibilità di modificarli e memorizzarli in modo da poterli sfruttare per *Usage Control*.

Gli *Status Attribute* vengono inizialmente definiti nel PAS, ed avranno un tipo, un identificatore ed eventualmente un valore. Per esempio uno *Status Attribute* definito in questo modo (*boolean isWriting = false*) codifica un attributo di stato di tipo booleano chiamato "isWriting" ed inizializzato a false.

Come detto prima bisogna avere la possibilità di modificare questi

nuovi attributi, e per questo sono state aggiunte delle *Pep Action*, ovvero delle azioni eseguite dal PEP in seguito alla valutazione di *Obligations*.

add(Attribute, int) e *add(Attribute, float)*

Questa *Pep Action* permette, in seguito alla valutazione di una *Obligations*, l'aggiunta di un valore numerico ad uno *Status Attribute* di tipo float o int. Effettuare questa operazione su un tipo non permesso porterà ad un errore in fase di valutazione.

```
obl:
    [permit M add(counter, 2)]
```

Per esempio l'esecuzione di questa *Obligation* su un'attributo, chiamato *counter*, inizializzato a 0, porterà l'attributo al valore 2. Mentre l'esecuzione di questo

```
obl:
    [permit M add(counter, "foo")]
```

porterà ad un errore per incoerenza sul tipo.

sub(Attribute, int) e *sub(Attribute, float)*

Questo insieme *Pep Actions* è semplicemente il duale della precedente, ciò vuol dire che invece che effettuare la somma di un valore numerico ad uno *Status Attribute* farà una sottrazione.

Quindi, riprendendo l'esempio citato per la add:

```
obl:
    [permit M sub(counter, 2)]
```

l'esecuzione corretta di questa *Obligation* porterà nuovamente l'attributo ad il suo valore originale, ovvero 0. Ovviamente riguardo gli errori vale lo stesso discorso fatto in precedenza.

div(Attribute, int) e *div(Attribute, float)*

Le *Pep Actions* di questa categoria effettuano una divisione tra un attributo ed un numero passato come parametro.

```
obl:
    [permit M div(number, 2)]
```

Presupponendo che il valore dell'attributo *number* sia inizialmente 6 l'esecuzione di questa operazione lo porterà a 6/2, ovvero 3.

mul(Attribute, int) e *mul(Attribute, float)*

Quest'azione, come facilmente intuibile dal nome effettua la moltiplicazione. Considerando l'esempio fatto per la div

```
obl:
    [permit M mul(number, 3)]
```

Visto che il valore dell'attributo, modificato in precedenza dalla div, è 3 l'operazione effettuata sarà $3 * 3$ che darà come risultato 9.

flag(Attribute, boolean)

Quest'operazione, definita solo sul tipo boolean modifica il valore di uno *Status Attribute* di tipo booleano.

```
obl:
    [permit M flag(isFoo, true)]
```

L'esecuzione con successo di questa *Obligation* porterà l'attributo *flag* ad avere un valore true.

sumDate(Attribute, date)

Anche questa azione, come quella di prima è definita su un solo tipo, ma questa volta il tipo è Date. Il tipo Date può essere espresso con in tre forme diverse

- HH:mm:ss
- yyyy/MM/dd
- yyyy/MM/dd-HH:mm:ss

Per fare un altro esempio consideriamo uno *Status Attribute* di tipo date inizializzato al giorno 2016/04/20 di nome *foo*.

```
obl:
    [permit M sumDate(foo, 24:00:00)]
```

La corretta esecuzione di questa *Obligation* porterà il valore di *foo* al giorno successivo, ovvero il 21 Aprile 2016.

sumString(Attribute, string)

L'operazione ora descritta coinvolge il tipo *string*. Passandogli un attributo di tipo *String* ed una stringa effettuerà la concatenazione.

```
obl:
    [permit M sumString(Pablo, " Neruda")]
```

Se l'attributo *Pablo* avesse il valore "*Pablo*", il risultato di questa operazione farebbe cambiare valore all'attributo in "*Pablo Neruda*".

setValue(Attribute, string)

Quest'operazione è molto simile alla precedente, ma invece che concatenare le stringhe sostituisce il valore presente dentro l'attributo con quello passatogli come parametro.

```
obl:
    [permit M setValue(Pablo, "Aghiò Aghiò")]
```

Quindi l'esecuzione corretta di quest'azione porterà l'attributo che precedentemente aveva il valore "*Pablo Neruda*" ad avere il valore "*Aghiò Aghiò*".

setDate(Attribute, date)

Quest'operazione è uguale alla precedente, ma invece che operare sul tipo *stringa* opera sul tipo *Data*.

```
obl:
    [permit M setDate(foo, 1993/09/24)]
```

L'esecuzione di questa *Obligation* modificherà il valore di *foo* al 24 Settembre 1993.

4.4 ESEMPI

Queste nuove funzionalità introdotte servono allo scopo descritto in sezione 2.2, ovvero l'implementazione di un nuovo modello chiamato *Usage Control*. Mostriamo ora l'implementazione in FACPL dei due esempi trattati in sezione 2.2.

4.4.1 Accesso ai file

Codice 4.2: Primo esempio

```

PolicySet ReadWrite_Policy { deny- unless- permit
  target: equal ( "Bob" , name / id ) && ("Alice, name/id")
  policies:
  PolicySet Write_Policy { deny- unless- permit
    target: equal("file", file/id) && ("write", action/id)
    policies:
      Rule write ( permit target:
        equal ( status / isWriting , false ) &&
        equal ( status / counterReadFile1, 0)
      )
    obl:
    [ permit M flagStatus(isWriting, true) ]
  }
  PolicySet Read_Policy { deny- unless- permit
    target: equal("file", file/id) && ("read", action/id)
    policies:
      Rule read ( permit target:
        equal ( status / isWriting , false ) &&
        less-than (status / counterReadFile1, 2)
      )
    obl:
    [ permit M addStatus(counterReadFile1, 1) ]
  }
  PolicySet StopWrite_Policy { deny- unless- permit
    target: equal("file", file/id) && ("stopWrite", action/id)
    policies:
      Rule stopWrite ( permit target:
        equal ( status / isWriting , true )
      )
    obl:
    [ permit M flagStatus(isWriting, false) ]
  }

```

```

}
PolicySet StopRead_Policy { deny- unless- permit
  target: equal("file", file/id) && ("stopRead", action/id)
  policies:
    Rule stopRead ( permit target:
      greater-than ( status / counterReadFile1 , 0 )
    )
    obl:
      [ permit M subStatus(counterReadFile1, 1) ]
  }
}
PAS {
  Combined Decision : false ;
  Extended Indeterminate : false ;
  Java Package : "example" ;
  Requests To Evaluate : Request1, Request2, Request3, Request4,
    Request5, Request6 ;
  pep: deny- biased
  pdp: deny- unless- permit
  status: [(boolean isWriting = false), (int counterReadFile1 = 0), ]
  include example
}

```

Per semplicità, in questo codice, vengono mostrate le policy di accesso per un solo file. Il primo esempio in sezione 2.2 poneva una regola sull'accesso ai file, ovvero permetteva un massimo di due persone in contemporanea che potevano effettuare l'accesso in lettura oppure un massimo di una persona che poteva ottenere l'accesso in scrittura.

Tutte le policy del codice 4.2 sono chiuse in un *PolicySet*. Il target del *PolicySet* *ReadWrite_Policy* verifica che le richieste provengano da utenti che hanno nome *Alice* o *Bob*, in caso contrario il responso sarà *Not Applicable*.

Successivamente sono state create quattro policy per gestire le quattro operazioni possibili, ovvero *read*, *write*, *stopRead* ed infine *stopWrite*.

Prendiamo in considerazione la prima policy, quella per la *write*. Come prima è presente un target, che richiede questa volta due diverse condizioni, la prima riguarda l'id del file richiesto, la seconda invece richiede che l'azione sia *write*. Le parti interessanti di questa policy sono

due, la prima riguarda la *Rule*, la seconda la *Obligation*.

La *Rule* restituisce `permit` se le due condizioni dell'equal sono vere, come si può facilmente notare l'operazione di confronto non viene fatta tra una stringa ed un normale attributo, ma tra una stringa ed uno *Status Attribute*.

L'ultima cosa da notare è l'unica *Obligation* presente per questa policy. Questo tipo particolare di *Obligation*, ha sempre al suo interno un'azione che verrà eseguita dal PEP, questa volta però non sarà una semplice azione come scrivere un log o mandare una mail, l'azione andrà a modificare lo stato del sistema, mettendo il valore `true` all'attributo *isWriting*.

Prendiamo ora una serie di richieste.

Codice 4.3: Richieste del primo esempio

```
Request:{ Request1
  (name / id , "Alice")
  (action / id, "read")
  (file / id, "file1")
}

Request:{ Request2
  (name / id , "Bob")
  (action / id, "Write")
  (file / id, "file1")
}

Request:{ Request3
  (name / id , "Bob")
  (action / id, "read")
  (file / id, "file1")
}

Request:{ Request4
  (name / id , "Alice")
  (action / id, "stopRead")
  (file / id, "file1")
}

Request:{ Request4
  (name / id , "Bob")
  (action / id, "stopRead")
```

```

    (file / id, "file1")
}

Request:{ Request6
  (name / id , "Alice")
  (action / id, "write")
  (file / id, "file1")
}

```

L'output di queste richieste sarà il seguente

```

Request1:
  PDP Decision=
    Decision: PERMIT
    Obligations: PERMIT M AddStatus([INT/counterReadFile1/0, 1])
  PEP Decision= PERMIT
Request2:
  PDP Decision=
    Decision: DENY Obligations:
  PEP Decision= DENY
Request3:
  PDP Decision=
    Decision: PERMIT
    Obligations: PERMIT M AddStatus([INT/counterReadFile1/1, 1])
  PEP Decision= PERMIT
Request4:
  PDP Decision=
    Decision: PERMIT
    Obligations: SubStatus([INT/counterReadFile1/2, 1])
  PEP Decision= PERMIT
Request5
  PDP Decision=
    Decision: PERMIT
    Obligations: PERMIT M SubStatus([INT/counterReadFile1/1, 1])
  PEP Decision= PERMIT
Request6:
  PDP Decision=
    Decision: PERMIT
    Obligations: PERMIT M FlagStatus([BOOLEAN/isWriting/false, true])
  PEP Decision= PERMIT

```

Analizziamo ora il motivo di queste decisioni. Nella prima richiesta ovviamente nessuno sta leggendo o scrivendo, quindi viene tranquillamente

restituito permit. Visto che è presente una *obligation* lo stato verrà aggiornato, sommando un'unità al contatore di letture. Alla seconda richiesta l'utente richiede la scrittura, che gli viene negata perché c'è già qualcuno che sta leggendo, però lo stesso utente effettua un'altra richiesta, questa volta in lettura, che gli viene concessa.

La quarta e la quinta richiesta vengono fatte per avvisare il sistema che la lettura è terminata, ovviamente la risposta è permit, e la *obligation* corrispondente decrementerà il contatore. La sesta ed ultima richiesta è una scrittura, che questa volta viene permessa, poiché nessuno sta scrivendo o leggendo.

4.4.2 Noleggio e acquisto di contenuti

In questo secondo esempio analizzeremo il caso di un'azienda di distribuzione di contenuti multimediali che vuole regolare l'accesso di quest'ultimi attraverso policy. Faremo un breve esempio con un solo file e due utenti, uno dei due utenti comprerà il file, l'altro lo noleggerà a tempo determinato. Nel codice 4.4 vengono mostrate solo una parte delle policy presenti nel codice completo A.1 mostrato in Appendice A.

Codice 4.4: Secondo Esempio

```

PolicySet Negozio { deny- unless- permit
  target: equal ( "Bob" , name / id ) || ( "Alice, name/id" )
  policies:

  PolicySet Buy_Policy { deny- unless- permit
    target: equal("file1", file/id) && ("buy", action/id)
    policies:
      Rule alice_buy ( permit target: (
        equal ( action / id , "buy" ) &&
        equal ( name / id, "Alice" ))
        obl:
          [ permit M setString("accessTypeAlice", "BUY") ]
        )
      Rule bob_buy ( permit target: (
        equal ( action / id , "buy" ) &&
        equal ( name / id, "Alice" ))
        obl:
          [ permit M setString("accessTypeBob", "BUY") ]
        )
  
```



```

}

PolicySet NUMBER_Policy { deny- unless- permit
  target: equal("file1", file/id) && ("number", action/id)
  policies:
    Rule alice_buy ( permit target: (
      equal ( action / id , "number" ) &&
      equal ( name / id, "Alice" ))
    obl:
      [ permit M setString("accessTypeAlice", "NUMBER") ]
      [ permit M addStatus("aliceFileIviewNumber", 2) ]
    )
    Rule bob_buy ( permit target: (
      equal ( action / id , "number" ) &&
      equal ( name / id, "Alice" ))
    obl:
      [ permit M setString("accessTypeBob", "NUMBER") ]
      [ permit M addStatus("bobFileIviewNumber", 2) ]
    )
  }

```

Queste due policy, e anche le altre che non sono state mostrate, sono racchiuse tutte all'interno del *Policy Set* Negozio il quale come prima cosa verifica se chi ha fatto la richiesta ha un determinato nome, in questo caso *Bob* o *Alice*.

Successivamente, se uno dei due effettua la richiesta di BUY, ovvero l'acquisto senza alcun tipo di limitazione, si entra nella prima policy e, tramite le *Obligation* si cambia l'attributo di stato. Invece se un utente decidesse di effettuare il noleggio con la modalità dove si limita il numero di visioni si entrerebbe nella seconda *Policy Set* la quale, attraverso *Obligations* aumenterà il numero di visioni di due unità. Analogo è il caso del noleggio a tempo.

Per disciplinare la visione è presente un altro *Policy Set*, mostrato anch'esso parzialmente in codice 4.5.

Codice 4.5: Secondo Esempio

```

PolicySet VIEW { deny- unless- permit
  target: equal("file1", file/id) && ("view", action/id)
  policies:
    Rule buy ( permit target: (

```

```

    equal ( status / accessTypeBob , "BUY" ) &&
    equal ( status / accessTypeAlice, "BUY"))
  )
  Rule number_alice (  permit target: (
    equal ( status / accessTypeAlice, "NUMBER" ) &&
    equal ( name / id, "Alice") && greater-than( status /
      aliceFileIviewNumber, 0))
    obl:
    [  permit M  subStatus("aliceFileIviewNumber", 1) ]
  )

```

Mostriamo ora in Codice 4.6 alcune richieste che possono essere fatte al sistema ed analizziamo le risposte che produrranno.

Codice 4.6: Richieste del Secondo Esempio

```

Request:{ Request1
  (name / id , "Alice")
  (action / id, "view")
  (file / id, "file1")
}

Request:{ Request2
  (name / id , "Bob")
  (action / id, "view")
  (file / id, "file1")
}

Request:{ Request3
  (name / id , "Alice")
  (action / id, "Buy")
  (file / id, "file1")
}

Request:{ Request4
  (name / id , "Alice")
  (action / id, "view")
  (file / id, "file1")
}

Request:{ Request4
  (name / id , "Bob")
  (action / id, "Time")
  (file / id, "file1")
}

```

```
}
```

```
Request:{ Request6  
  (name / id , "Bob")  
  (action / id, "view")  
  (file / id, "file1")  
}
```

La prima e la seconda richiesta sono richieste di visione, che ovviamente restituiranno entrambe deny, in quanto nessun utente ha effettuato acquisti o noleggi. Successivamente Alice effettuerà un acquisto ed una visione ed entrambi andranno a buon fine. A questo punto Bob, a cui prima era stata negata la visione effettuerà una richiesta di noleggio e dopo una richiesta di visione, il risultato di entrambe sarà permit.

Tabella 3.: Sintassi di FACPL_{PB}

Policy Authorisation Systems	$PAS ::= (\text{pep} : \text{EnfAlg} \text{ pdp} : \text{PDP} (\text{status} : [\text{Attribute}]^+)^*)$
Attribute	$\text{Attribute} ::= (\text{Type Identifier} (= \text{Value})^?)$
Type	$\text{Type} ::= \text{int} \mid \text{boolean} \mid \text{date} \mid \text{float}$
Enforcement algorithms	$\text{EnfAlg} ::= \text{base} \mid \text{deny-biased} \mid \text{permit-biased}$
Policy Decision Points	$\text{PDP} ::= \{\text{Alg} \text{ policies} : \text{Policy}^+\}$
Combining algorithms	$\text{Alg} ::= \text{p-over}_\delta \mid \text{d-over}_\delta \mid \text{d-unless-p}_\delta \mid \text{p-unless-d}_\delta$ $\mid \text{first-app}_\delta \mid \text{one-app}_\delta \mid \text{weak-con}_\delta \mid \text{strong-con}_\delta$
fulfilment strategies	$\delta ::= \text{greedy} \mid \text{all}$
Policies	$\text{Policy} ::= (\text{Effect} \text{ target} : \text{Expr} \text{ obl} : \text{Obligation}^*)$ $\mid \{\text{Alg} \text{ target} : \text{Expr}$ $\text{policies} : \text{Policy}^+ \text{ obl} : \text{Obligation}^*\}$
Effects	$\text{Effect} ::= \text{permit} \mid \text{deny}$
Obligations	$\text{Obligation} ::= [\text{Effect} \text{ ObType} \text{ PepAction}(\text{Expr}^*)]$
PepAction	$\text{PepAction} ::= \text{add}(\text{Attribute}, \text{int}) \mid \text{flag}(\text{Attribute}, \text{boolean})$ $\mid \text{sumDate}(\text{Attribute}, \text{date}) \mid \text{div}(\text{Attribute}, \text{int})$ $\mid \text{add}(\text{Attribute}, \text{float}) \mid \text{mul}(\text{Attribute}, \text{float})$ $\mid \text{mul}(\text{Attribute}, \text{int}) \mid \text{div}(\text{Attribute}, \text{float})$ $\mid \text{sub}(\text{Attribute}, \text{int}) \mid \text{sub}(\text{Attribute}, \text{float})$ $\mid \text{sumString}(\text{Attribute}, \text{string})$ $\mid \text{setValue}(\text{Attribute}, \text{string})$ $\mid \text{setDate}(\text{Attribute}, \text{date})$
Obligation Types	$\text{ObType} ::= \text{M} \mid \text{O}$
Expressions	$\text{Expr} ::= \text{Name} \mid \text{Value}$ $\mid \text{and}(\text{Expr}, \text{Expr}) \mid \text{or}(\text{Expr}, \text{Expr}) \mid \text{not}(\text{Expr})$ $\mid \text{equal}(\text{Expr}, \text{Expr}) \mid \text{in}(\text{Expr}, \text{Expr})$ $\mid \text{greater-than}(\text{Expr}, \text{Expr}) \mid \text{add}(\text{Expr}, \text{Expr})$ $\mid \text{subtract}(\text{Expr}, \text{Expr}) \mid \text{divide}(\text{Expr}, \text{Expr})$ $\mid \text{multiply}(\text{Expr}, \text{Expr}) \mid \text{less-than}(\text{Expr}, \text{Expr})$
Attribute Names	$\text{Name} ::= \text{Identifier/Identifier} \mid \text{Status/Identifier}$
Literal Values	$\text{Value} ::= \text{true} \mid \text{false} \mid \text{Double} \mid \text{String} \mid \text{Date}$
Requests	$\text{Request} ::= (\text{Name}, \text{Value})^+$

ESTENSIONE DELLA LIBRERIA FACPL

Il linguaggio FACPL è basato interamente su una libreria scritta in Java. Per implementare la valutazione di richieste basate sul comportamento passato è stato necessario estendere questa libreria con nuove classi e modificarne alcune.

In questo capitolo verranno mostrate le novità introdotte nel capitolo 4 sotto il punto di vista implementativo, per ovvi motivi verranno mostrate solo alcune parti delle modifiche effettuate, ma il codice completo si può comunque trovare su GitHub.

5.1 ESTENSIONE DELLE CLASSI

Il primo passo per l'estensione della libreria è stato l'implementazione di uno *Status* e degli *Status Attribute* mostrati in Figura 10. La dipendenza tra queste classi è dovuta ad una lista di attributi mantenuta dallo stato.

Ovviamente questi attributi vanno in qualche modo comparati, in questo caso sono stati modificati i comparatori già presenti mostrati in Figura 11. La modifica ha coinvolto le classi derivanti dall'interfaccia *IComparisonFunction*, ed è stata la semplice aggiunta di un metodo. Successivamente è stato necessario trovare un modo di modificare questi attributi in modo tale da soddisfare il requisito di dinamismo richiesto da *Usage Control*. Per questo motivo sono state introdotte delle funzioni già citate in Sezione 4.2 e Sezione 4.3. Per l'implementazione è stata necessaria una nuova gerarchia di classi mostrata in Figura 12. La struttura somiglia molto a quella dei comparatori, ovvero un factory che restituisce un valutatore, nel quale sono definite le vere e proprie funzioni, e le varie operazioni, derivanti tutte da un'interfaccia comune, che eseguono l'operazione chiamando il metodo sul valutatore passatogli in base al

tipo dell'attributo.

Successivamente è stato esteso il contesto in maniera tale che lo *Status* possa essere preso in considerazione dal PDP durante il processo di valutazione, andando così ad influenzarne le decisioni, ed in Figura 13 si può vedere come è stato esteso. La prima classe coinvolta dall'estensione è stata il *ContextStub*, introducendo una nuova sottoclasse che ingloba uno *Status* e di conseguenza permette di ricavarne gli *Status Attribute*. La seconda modifica ha coinvolto la classe che fa da tramite tra la richiesta ed il contesto, ed anche in questo caso è stata semplicemente introdotta una nuova classe sulla quale sono definiti metodi specifici per gli *Status Attribute*.

L'ultima parte del lavoro è consistita nel implementare un nuovo tipo di *Obligation*, chiamate *ObligationStatus*, e modificare il PEP in modo che ne potesse effettuare il *discharge*. Le modifiche apportate sono mostrate in Figura 14. Per implementare le *ObligationStatus* è stato necessario estendere due gerarchie differenti, la prima è quella delle *Obligation* a livello sintattico, dove è stato creato un nuovo tipo che contenesse al suo interno una funzione capace di modificare uno *Status Attribute*. La seconda gerarchia riguarda invece le *Obligation* pronte per essere valutate, anche in questo caso la modifica è stata analoga a quella fatta per quelle a livello sintattico permettendo così a quest'ultime di contenere un'azione capace di modificare lo stato. Modificare il PEP non è stato difficile, è stato necessario semplicemente aggiungere al metodo che effettua il processo di *Enforcement* poche righe di codice in modo tale che prendesse in considerazione anche le nuove *Obligation* ed eseguisse l'operazione al loro interno.

5.2 STATUS E STATUS ATTRIBUTE

Il primo passo per estendere la libreria è stato la creazione di uno *Status*, che è modellato da una semplice classe di cui ne verrà mostrato un pezzo nel codice 5.1, successivamente sono stati creati gli *Status Attribute*, il codice completo è mostrato in Sezione A.2.1. La relazione che intercorre tra queste nuove classi è mostrata in Figura 10.

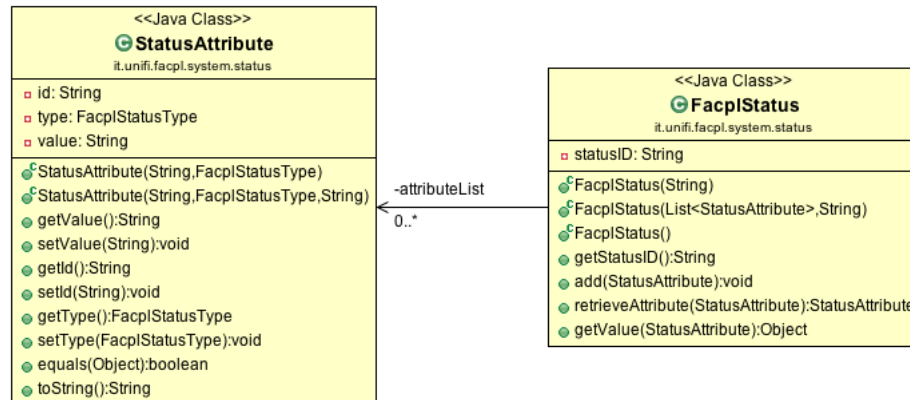


Figura 10.: Grafico UML delle classi Status e StatusAttribute

A livello implementativo invece verranno mostrati solo dei piccoli pezzi di codice.

Codice 5.1: Stralcio della classe Status

```

public class FacplStatus {
2   private List<StatusAttribute> attributeList;
   private String statusID;
4   public FacplStatus(String statusID) {
       attributeList = new ArrayList<StatusAttribute>();
6       this.statusID = statusID;
   }
8   public FacplStatus(List<StatusAttribute> attributeList, String
       statusID) {
       this.attributeList = attributeList;
10      this.statusID = statusID;
   }
12  public FacplStatus() {
       attributeList = new ArrayList<StatusAttribute>();
14      this.statusID = UUID.randomUUID().toString().substring(0, 8);
   }
}
  
```

Questa classe ha un campo essenziale per la logica del sistema, ed è una *LinkedList* di *Status Attribute*. In questa classe, oltre ad i costruttori ed alcuni getter sono stati implementati due metodi mostrati in Codice 5.2, uno per andare a cercare lo *Status Attribute*, e l'altro per restituirne il valore.

Codice 5.2: Metodi per gli *Status Attribute*

```

1  public StatusAttribute retrieveAttribute(StatusAttribute
    attribute) throws MissingAttributeException {
    int i = this.attributeList.indexOf(attribute);
3   if (i != -1) {
        return this.attributeList.get(i);
5   } else {
        throw new MissingAttributeException("attribute doesn't exist in the
            current status");
7   }
    }
9  public Object getValue(StatusAttribute attribute) throws
    MissingAttributeException {
    return (Object) (this.retrieveAttribute(attribute).getValue());
11 }

```

Gli *Status Attribute* sono modellati da una singola classe, anch'essa molto breve e facile da capire. Come facilmente intuibile dai costruttori in Codice 5.3 questa classe ha tre campi, un id, un valore, ed un tipo.

Codice 5.3: Costruttori di Status Attribute

```

    public StatusAttribute(String id, FacplStatusType type) {
2      this.id = id;
        this.type = type;
4      if (type == (FacplStatusType.INT) || type ==
            (FacplStatusType.DOUBLE)) {
            value = "0";
6      } else if (type == FacplStatusType.BOOLEAN) {
            value = "false";
8      } else if (type == FacplStatusType.DATE) {
            value = "0";
10     } else {
            value = "";
12     }
    }
14  public StatusAttribute(String id, FacplStatusType type, String
        value) {
        this.id = id;
16     this.type = type;
        this.value = value;
18  }

```

Il senso del secondo costruttore è facilmente intuibile, mentre il primo è

stato creato appositamente per dare un valore di default all'attributo nel caso non venisse inizializzato.

5.3 IMPLEMENTAZIONE DEI COMPARATORI SUGLI STATUS ATTRIBUTE

Nella libreria di FACPL era già presente una solida struttura (Figura 11), basata su un factory, per la comparazione di attributi, quindi è bastato modificare le varie funzioni in modo tale che potessero operare anche su *Status Attribute*. Prendendo in esame la funzione *Equals* vediamo come funziona ora, a livello implementativo, il processo di comparazione.

Codice 5.4: Classe che implementa Equal

```
private Object convertType(StatusAttribute sa) {  
2   if (sa.getType() == FacplStatusType.BOOLEAN) {  
       if (sa.getValue() == "true") {  
4         return true;  
       } else  
6         return false;  
   } else if (sa.getType() == FacplStatusType.DOUBLE) {  
8     return (Double)Double.parseDouble(sa.getValue());  
   } else if (sa.getType() == FacplStatusType.INT) {  
10    return (Integer)Integer.parseInt(sa.getValue());  
   } else if (sa.getType() == FacplStatusType.STRING) {  
12    return sa.getValue();  
   }  
14   return null;  
   }  
16 }
```

Vedendo il codice A.4 si nota che la classe implementa un'interfaccia, quest'ultima definisce al suo interno un unico metodo astratto, *public Boolean evaluateFunction(List<Object> args)* che sarà il metodo chiamato in fase di valutazione. La modifica del processo di comparazione è stata fatta in questo metodo, bisognava fare in modo che uno, o entrambi gli argomenti, potessero essere *Status Attribute*, e per questo è stata introdotta un'altra funzione, chiamata *convertType*, mostrata in Codice 5.4, che dato uno *Status Attribute*, va a ricavarne il valore.

Quando verrà richiamato il primo metodo verrà effettuato un controllo

sul tipo dell'argomento, e in base a questo risultato verrà chiamato il secondo metodo che effettuerà l'operazione descritta in precedenza.

5.4 FUNZIONI PER LA MODIFICA DEGLI STATUS ATTRIBUTE

Per concetto di *Status Attribute* è richiesto dinamismo, in quanto devono irrimediabilmente cambiare rispetto alla valutazione di una richiesta, quindi sono state implementate funzioni che effettuano queste operazioni di modifica.

Per mantenere la coerenza con il resto della libreria queste funzioni sono state implementate in modo simile a come sono state implementate quelle di comparazione, motivo per cui l'UML in Figura 12 somiglia molto a quello usato per la comparazione. Ora verrà mostrato il caso di operazioni numeriche. Sono state implementate anche operazioni su stringhe, ma il funzionamento è analogo alla sua controparte numerica.

Come si nota dalla Figura 12 tutto parte da un interfaccia, che dovrà essere implementata da tutte le funzioni che andranno a modificare lo stato, quest'ultima è composta da un solo metodo che verrà chiamato per l'esecuzione dell'operazione.

Codice 5.5: Interfaccia per le operazioni

```

public interface IExpressionFunctionStatus {
2
    public void evaluateFunction(List<Object> args) throws Throwable;
4
}

```

In questo caso, da quest'interfaccia deriva una classe astratta per le operazioni aritmetiche che implementerà il metodo astratto dell'interfaccia ed aggiungerà un altro metodo astratto, che rappresenterà la funzione vera e propria.

Codice 5.6: Metodo implementato dall'interfaccia

```

1  public void evaluateFunction(List<Object> args) throws Throwable {
    if (args.size() == 2) {
2      StatusAttribute s1;
3      if (args.get(0) instanceof StatusAttribute) {
5          s1 = (StatusAttribute) args.get(0);
        } else {

```

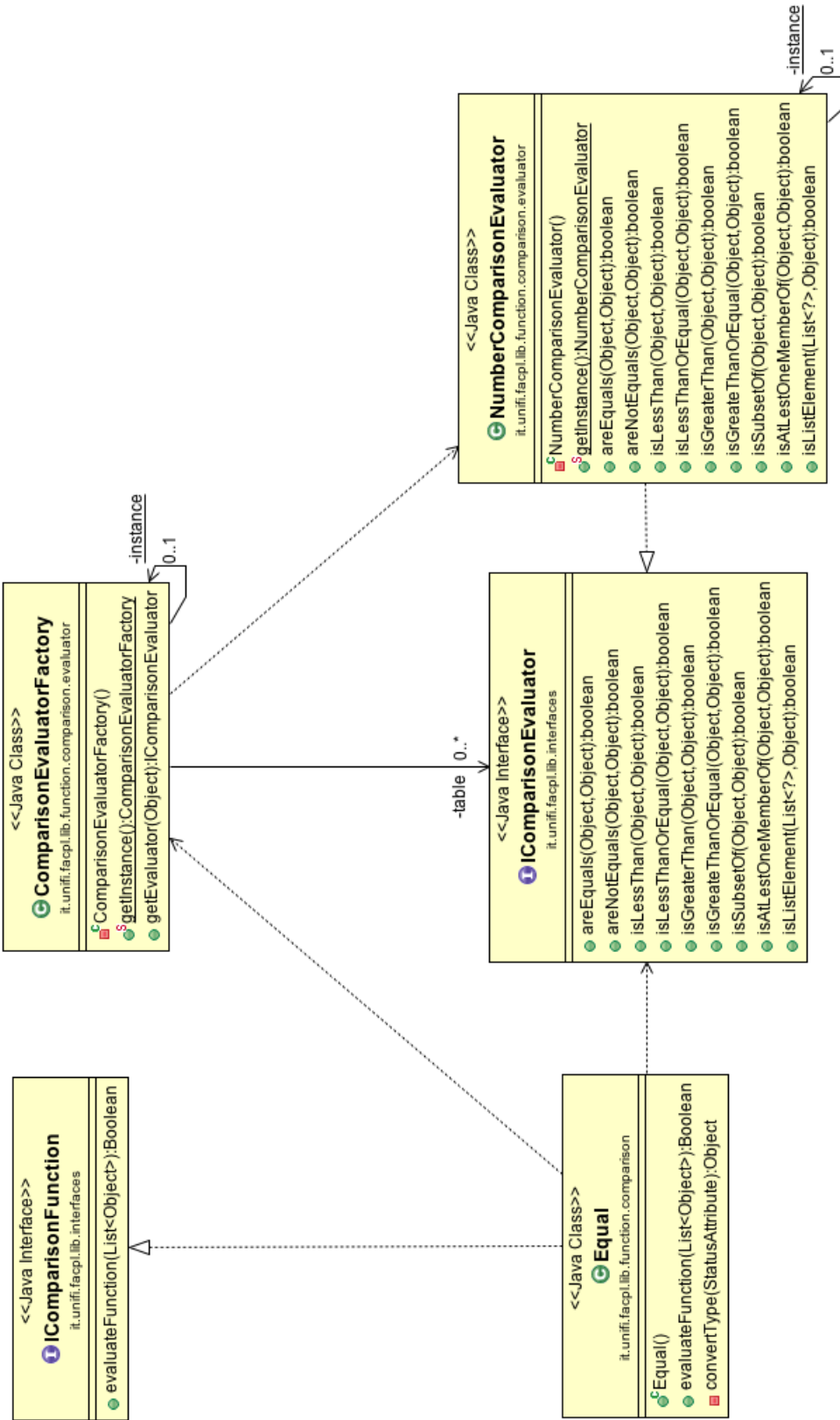


Figura 1.1.: Grafico UML per la gerarchia di classi usate nella comparazione

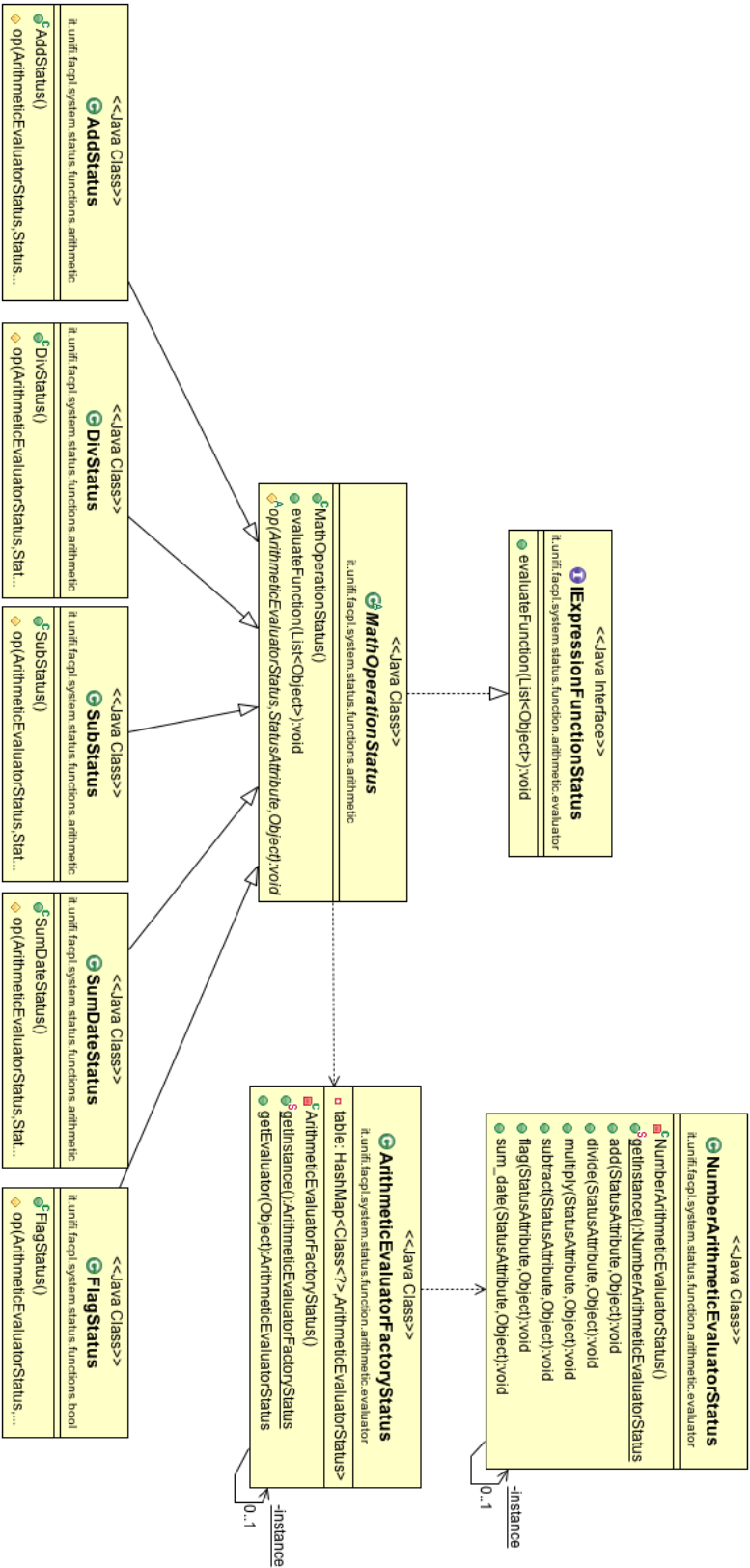


Figura 12.: Grafico UML per la gerarchia di funzioni aritmetiche

```
7         throw new Exception("First argument it's not a Status Attribute");
      }
9      Object o2 = args.get(1);
      ArithmeticEvaluatorStatus evaluator =
          ArithmeticEvaluatorFactoryStatus.getInstance().getEvaluator(o2);
11      op(evaluator, s1, o2);
      } else {
13         throw new Exception("Illegal number of arguments");
      }
15 }
```

Dal questo codice si notano subito molte somiglianze con quello proposto in sezione 5.3, questo perché la logica di funzionamento è sostanzialmente la stessa. Inizialmente viene effettuato un controllo sul tipo degli argomenti, successivamente viene richiesto un valutatore corretto per il tipo di dato passatogli e poi è effettuata l'operazione chiamando il metodo *op*, che sfruttando il principio del pattern Template, è implementato nelle varie sottoclassi differenziando così il comportamento senza dover riscrivere interamente il metodo, risparmiando così molte righe di codice.

Le classi che estendono *MathOperationStatus* sono molto simili tra di loro, quindi prenderemo in esame solo la classe che effettua l'operazione di somma, mostrata in basso a sinistra nella Figura 12.

Codice 5.7: Classe per la somma

```
1 public class AddStatus extends MathOperationStatus {
2
3     @Override
4     protected void op(ArithmeticEvaluatorStatus ev, StatusAttribute
        s1, Object o2) throws Throwable {
5         ev.add(s1, o2);
6     }
7 }
```

Questa classe implementa semplicemente il metodo astratto, chiamando sul valutatore passatogli in precedenza la funzione di somma.

Il valutatore non è altro che una classe che implementa tutte le operazioni di una determinata categoria, per esempio in questo caso viene restituito un valutatore che effettua le operazioni aritmetiche. A puro scopo esemplificativo mostriamo ora come è implementata l'operazione

di somma nel valutatore aritmetico, il codice completo si può sempre visionare in Sezione A.2.3.

Codice 5.8: Metodo implementato dall'interfaccia

```

1  public void add(StatusAttribute o1, Object o2) throws Throwable {
    if (o1.getType() == FacplStatusType.INT) {
3      Integer value = Integer.parseInt(o1.getValue());
      Integer newValue = value + (int) o2;
5      o1.setValue(newValue.toString());
    } else if (o1.getType() == FacplStatusType.DOUBLE) {
7      Double value = Double.parseDouble(o1.getValue());
      Double newValue = value + (double) o2;
9      o1.setValue(newValue.toString());
    } else {
11     throw new UnsupportedOperationException("Number", "Add");
    }
13 }

```

5.5 ESTENSIONE DEL CONTESTO

Lo *Status* creato in 5.2 andrà in qualche modo preso in considerazione durante il processo di valutazione in modo che vada ad influenzare le decisioni. Di conseguenza lo stato dev'essere inglobato dal contesto in cui viene valutata la richiesta.

Per prima cosa è stato necessario estendere la gerarchia di classi derivanti dall'interfaccia *IContextStub*. Come si può vedere in figura 13 è stata fatta un'operazione di refactoring astraendo alcune parti in comune, ed è stata creata la classe *ContextStub_Default_Status* di cui ora ne verrà analizzata l'implementazione.

Come si nota dall'immagine 13 la classe è implementata come un *Singleton* e contiene diversi metodi legati a *Status*, uno di questi è il *Setter*, che permette di aggiungere lo stato, l'altro invece è un *Getter* che permette di ricavare un attributo dallo stato. Il metodo più importante invece è quello mostrato in Codice 5.9

Codice 5.9: Classe *ContextStub_Default_Status*

```

1  public Object getContextValues(Object attr) {
    try {
3      if (attr instanceof StatusAttribute) {

```

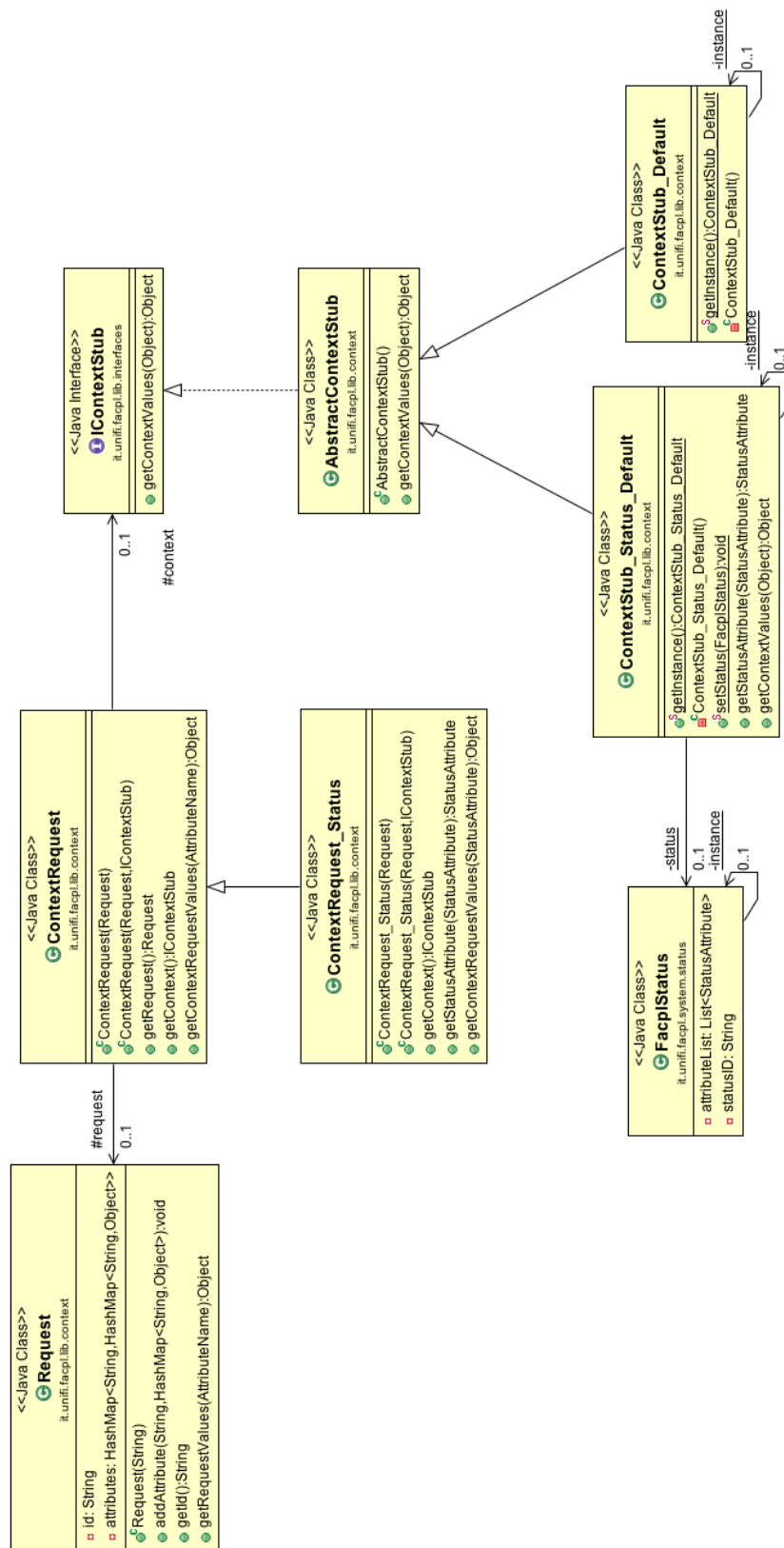


Figura 13.: Grafico UML del contesto

```

        return status.getValue((StatusAttribute) attr);
5      } else {
        return super.getContextValues(attr);
7      }
    } catch (MissingAttributeException e) {
9      return null;
    }
11 }
}

```

Questo metodo permette di effettuare la ricerca mostrata in Figura 9, ovvero datogli un attributo andrà prima a verificare la sua presenza all'interno dello *Status*, dopodiché se non lo trova verificherà la presenza all'interno dell'ambiente.

Successivamente è stata estesa anche alla classe *ContextRequest* con una nuova classe *ContextRequest_Status*, la cui unica differenza è un semplice *Getter* per gli attributi di stato.

5.6 OBLIGATIONS E PEP

Lo stato alla necessità andrà aggiornato, e qua entrano in gioco due componenti fondamentali del sistema, il PEP e le *Obligations*.

Anche in questo caso sono state estese le *Obligation* introducendo un nuovo tipo chiamato *Obligation Status*, questo tipo particolare di *Obligation* servono per andare ad eseguire azioni sullo stato. Nella libreria sono presenti due tipi fondamentali di *Obligation*, il primo sono quelle a livello sintattico, le seconde, chiamate *FulfilledObligations* sono quelle pronte ad essere valutate. Vediamo adesso come sono state estese quelle a livello sintattico.

Per eseguire questa estensione è stato reso necessario un refactoring, per prima cosa è stato astratto tutto il comportamento comune in una superclasse astratta, successivamente è stata creata la nuova classe che modella questo nuovo tipo. Il refactoring ha coinvolto anche il metodo che si occupa del *Fulfilling* delle *Obligation* in quanto ora deve creare anche questo nuovo tipo, la scelta più ovvia è stata creare un metodo astratto implementato nelle due sottoclassi che viene chiamato dalla superclasse per creare il tipo corretto.

Codice 5.10: Parte rifattorizzata del metodo che si occupa del fulfilling

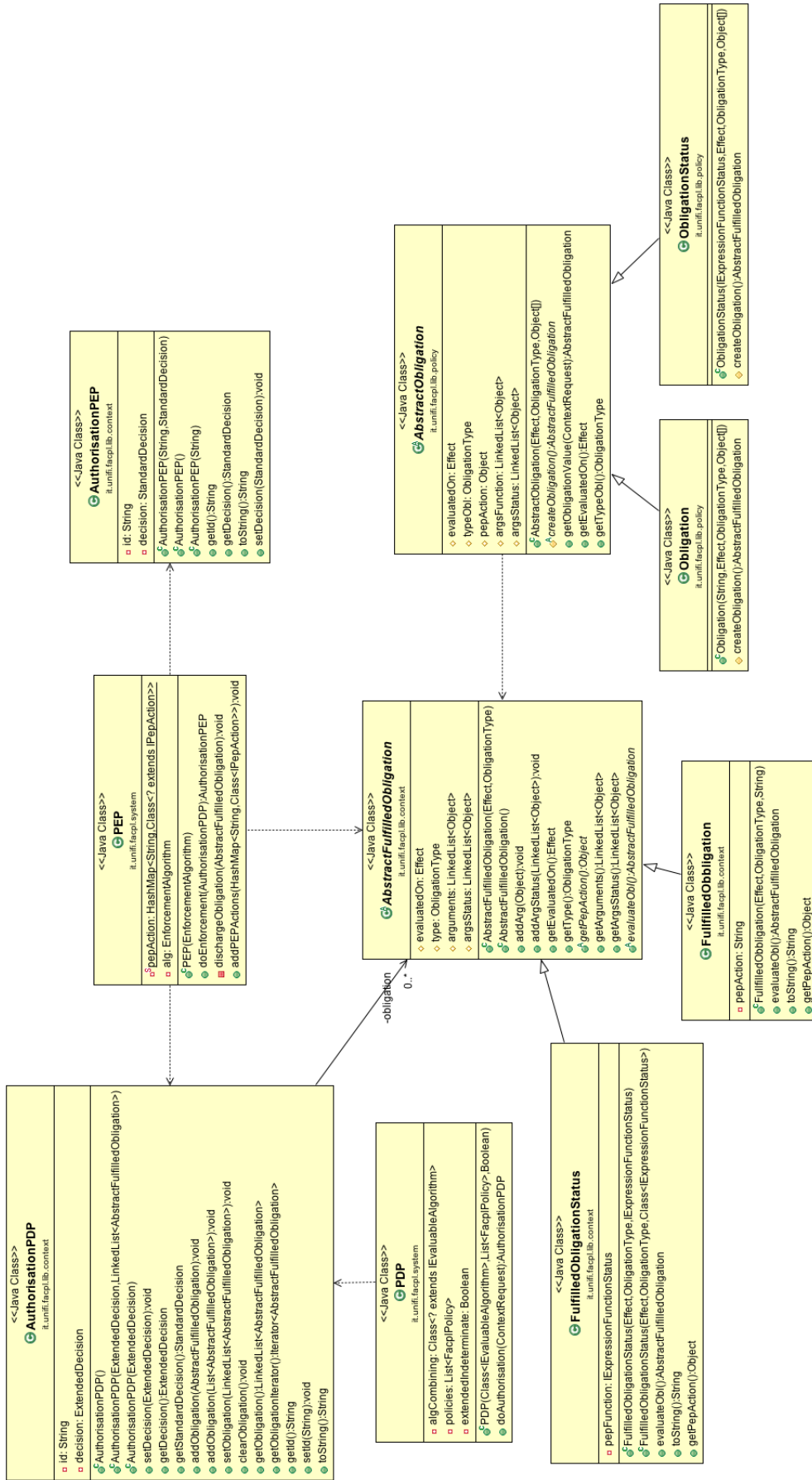


Figura 14.: Relazioni tra Obligation e PEP

```

    l.debug("Fulfilling Obligation " + this.pepAction.toString() + "...");
2   AbstractFulfilledObligation obl = this.createObligation();
    if (obl instanceof FulfilledObligationCheck) {

```

Codice 5.11: CreateObligation nelle status

```

protected AbstractFulfilledObligation createObligation() {
2   AbstractFulfilledObligation obl = new
        FulfilledObligationStatus(this.evaluatedOn, this.typeObl,
            (IExpressionFunctionStatus) this.pepAction);
4   if (!argsStatus.isEmpty()) {
        obl.addArgStatus(argsStatus);
6   }
    return obl;
8 }

```

Codice 5.12: CreateObligation nelle normali

```

@Override
2   protected AbstractFulfilledObligation createObligation() {
        return new FullfilledObbligation(this.evaluatedOn,
            this.typeObl, (String) this.pepAction);
4   }

```

La *Obligation* di stato necessiterà anche di argomenti su cui eseguire l'azione, che le verranno passati in fase di costruzione.

Alla fine della valutazione il PDP crea un oggetto di tipo *AuthorisationPDP* che conterrà la decisione e una lista di *FulfilledObligation*, quest'ultime poi andranno al PEP per la loro valutazione. Vediamo ora come sono state implementate.

Anche in questo caso è stato necessario un refactoring analogo a quello fatto per le prime.

Codice 5.13: Peculiarità della classe FulfilledObligationStatus

```

public class FulfilledObligationStatus extends
    AbstractFulfilledObligation {
2   private IExpressionFunctionStatus pepFunction;
    public FulfilledObligationStatus(Effect effect, ObligationType
        typeObl, IExpressionFunctionStatus pepFunction) {

```

```

4      super(effect, typeObl);
      this.pepFunction = pepFunction;
6  }
      public FulfilledObligationStatus(Effect effect, ObligationType
          typeObl,
8          Class<? extends IExpressionFunctionStatus> pepFunction) {
          super(effect, typeObl);
10     }
      @Override
12     public AbstractFulfilledObligation evaluateObl() throws Throwable
          {
              this.pepFunction.evaluateFunction(this.getArgsStatus());
14     return this;
          }

```

Come si può notare, in fase di costruzione, gli verrà passato un oggetto di tipo *IExpressionFunctionStatus* che sarà l'azione che andrà a eseguire sullo stato. Quest'azione andrà realmente ad essere eseguita quando verrà chiamato dal PEP il metodo *evaluateObl*.

Il PEP nella fase di enforcement effettua la valutazione delle *Obligation*, in questo caso le modifiche per permettere al sistema di eseguirle sono state minime, è bastato modificare il metodo *DischargeObligation* in modo che quando gli viene passata una *AbstractFulfilledObligation* chiamasse il metodo *evaluateObl*.

Codice 5.14: Discharge delle Fulfilled Obligation di stato

```

1      else if (obl instanceof FulfilledObligationStatus) {
          obl = (FulfilledObligationStatus) obl;
3          obl.evaluateObl();
      }

```

Il codice completo riguardante questa sezione è presente in Appendice A.2.4

5.7 PLUGIN DI ECLIPSE

[TODO: CORREGGERE PARTE SU XTEND E MAGARI ALLUNGARE]
 Il progetto è basato su Java, ed il codice formalizzato in FACPL viene successivamente convertito in codice Java attraverso un processo di autogenerazione. Per fare questo si usa un linguaggio chiamato XTend.



Figura 15.: Logo di Xtend

XTend ha le sue radici in Java, ma si concentra maggiormente su aspetti come una sintassi più concisa, ed altre funzionalità come l'inferenza sui tipi, l'overload degli operatori o l'estensione dei metodi (?). È principalmente un linguaggio *Object-oriented*, ma integra caratteristiche tipiche di un linguaggio funzionale, come ad esempio le Lambda Expression. Il sistema dei tipi di XTend è lo stesso di Java, ed è quindi statico.

5.8 ESEMPIO

In questa sezione verrà mostrato come sarà in Java il corrispettivo del Codice 4.2 e del Codice 4.3.

Tutto parte dalla classe dove è presente il metodo Main (Codice 5.15. In questo stesso modulo viene preparato il sistema all'esecuzione attraverso l'inizializzazione di tutti i componenti necessari al sistema.

I due componenti più importanti sono il PDP e il PEP che vengono inizializzati nel costruttore, in quest'ultimo vengono anche aggiunte le *Policy* e creato un contesto. Successivamente all'inizializzazione verranno inserite tutte le richieste in una lista e partirà un ciclo che effettuerà l'operazione di autorizzazione del PDP e di enforcement del PEP.

Codice 5.15: Main di uno scenario FACPL

```

public class MainFACPL {
2   private PDP pdp;
   private PEP pep;
4   public MainFACPL() throws MissingAttributeException {
       LinkedList<FacplPolicy> policies = new
           LinkedList<FacplPolicy>();
6   policies.add(new
       PolicySet_ReadWrite(ContextRequest_WriteRequestAlice.getContextReq()));
       this.pdp = new
           PDP(it.unifi.facpl.lib.algorithm.PermitUnlessDenyGreedy.class,
           policies, false);
8   this.pep = new PEP(EnforcementAlgorithm.DENY_BIASED);

```

```

        this.pep.addPEPActions(PEPAction.getPepActions());
10    }
    public static void main(String[] args) throws
        MissingAttributeException {
12        MainFACPL system = new MainFACPL();
        StringBuffer result = new StringBuffer();
14        LinkedList<ContextRequest_Status> requests = new
            LinkedList<ContextRequest_Status>();
        requests.add(ContextRequest_ReadRequestAlice.getContextReq());
16        requests.add(ContextRequest_WriteRequestBob.getContextReq());
        requests.add(ContextRequest_ReadRequestBob.getContextReq());
18        requests.add(ContextRequest_StopReadRequestAlice.getContextReq());
        requests.add(ContextRequest_StopReadRequestBob.getContextReq());
20        requests.add(ContextRequest_WriteRequestAlice.getContextReq());
        for (ContextRequest rcxt : requests) {
22            AuthorisationPDP resPDP = system.pdp.doAuthorisation(rcxt);
            AuthorisationPEP resPEP = system.pep.doEnforcement(resPDP);
24        }
    }
26 }

```

Per esigenze di comodità il contesto è stato integrato in un'unica classe insieme alle richieste.

Codice 5.16: Richiesta e contesto

```

public class ContextRequest_StopReadRequestAlice {
2    private static ContextRequest_Status CxtReq;
    public static ContextRequest_Status getContextReq() {
4        if (CxtReq != null) {
            return CxtReq;
6        }
        HashMap<String, Object> req_category_attribute_name = new
            HashMap<String, Object>();
8        HashMap<String, Object> req_category_attribute_action = new
            HashMap<String, Object>();
        HashMap<String, Object> req_category_attribute_file = new
            HashMap<String, Object>();
10        req_category_attribute_name.put("id", "Alice");
        req_category_attribute_action.put("id", "stopRead");
12        req_category_attribute_file.put("id", "file1");
        Request req = new Request("stop_read_request");
14        req.addAttribute("name", req_category_attribute_name);

```

```

    req.addAttribute("action", req_category_attribute_action);
16 req.addAttribute("file", req_category_attribute_file);
    CxtReq = new ContextRequest_Status(req,
        ContextStub_Status_Default.getInstance());
18 ContextStub_Status_Default.getInstance().setStatus(createStatus());
    return CxtReq;
20 }
    private static FacplStatus createStatus() {
22     ArrayList<StatusAttribute> attributeList = new
        ArrayList<StatusAttribute>();
        attributeList.add(new StatusAttribute("isWriting",
            FacplStatusType.BOOLEAN, "false"));
24 attributeList.add(new StatusAttribute("counterReadFile1",
            FacplStatusType.INT, "0"));
        attributeList.add(new StatusAttribute("counterReadFile2",
            FacplStatusType.INT, "0"));
26 FacplStatus status = new FacplStatus(attributeList, "stato");
        return status;
28 }
}

```

Il metodo che si occupa della creazione dello stato è *createStatus()*, il quale non farà altro che crearsi una serie di attributi ed inserirli in un nuovo oggetto di tipo *FacplStatus*, per poi restituirlo. La richiesta invece viene restituita sottoforma di un oggetto di tipo *ContextRequest_Status*, il quale verrà restituito dal primo dei due metodi. La richiesta è formata da diverse *HashMap* che sono come le categorie degli attributi che verranno inseriti al loro interno. Queste hashmap poi vengono aggiunte ad un oggetto *Request* insieme ad una stringa che racchiude l'informazione riguardante la categoria dell'oggetto appena inserito. Alice, in Codice 4.3, richiede ad un certo punto un'azione identificata come (*action / id* , "*stopRead*"), ed insieme a questo attributo manderà anche altri due attributi, uno che rappresenta il suo nome, e l'altro che contiene il nome del file su cui deve essere effettuata l'azione. L'attributo riguardante l'azione viene codificato alle righe 11 e 15.

Come ultima cosa vediamo come viene codificato un set di *Policy*. Come detto in precedenza una *Policy* è formata da un *Target*, eventualmente altre *Policy* o *Rule* e delle *Obligation*. Prendiamo ora in esempio una *Policy* che contiene tutti e tre questi elementi. Il codice di questa *Policy* è possibile trovarlo in A.11. In particolare è stata presa in considerazione la

Policy che permette di fermare la lettura, ovvero quella che verrà valutata quando verrà effettuata la richiesta in Codice 5.16.

Tutte le *Policy* derivano da una classe astratta che verrà estesa secondo le necessità. Come detto prima questa *Policy* contiene tutti e tre gli elementi che la caratterizzano, in particolare la *Obligation* che in questo caso è una *ObligationStatus*. Questa *Obligation* viene aggiunta come tutte le altre, ovvero chiamando l'apposito metodo della superclasse, ed è costruita passandogli come parametro un'azione da effettuare e gli argomenti, in questo caso l'azione è la sottrazione e gli argomenti è l'attributo che rappresenta il numero di lettori e l'intero 1.

Codice 5.17: Expression Function che valuta un attributo di stato

```

1      ExpressionFunction e1=new
      ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
      ctxReq.getStatusAttribute(
3          ctxReq.getStatusAttribute(new
              StatusAttribute("isWriting",
              FacplStatusType.BOOLEAN))),
      false);

```

Nel Codice 5.17 si può vedere come una *ExpressionFunction* riesca a valutare un attributo di stato.

CONCLUSIONI

Durante questa tesi è stata affrontato il lavoro di implementazione di *Usage Control* in FACPL. Come primo compito ci siamo occupati di analizzare i principali modelli dedicati all'*Access Control* e successivamente è seguita una fase di approfondimento sul modello *Usage Control* proposto da Sandhu e Park in [2].

Il lavoro è seguito con una disamina sul linguaggio FACPL in modo da comprendere al meglio la sintassi, la semantica e soprattutto il processo di valutazione così da avere un background e sapere come, e dove, intervenire per l'implementazione del concetto di *Status* e di tutte le cose che conseguentemente ne derivano da esso.

Prima di intervenire sulla libreria Java è stato necessario definire una sintassi estesa. Nella sintassi estesa sono state aggiunte nuove regole di produzione e ne sono state modificate alcune. Quelle modificate includono la definizione del sistema, mentre quelle aggiunte riguardano nuove funzioni, ed un nuovo tipo di attributo, chiamato *Status Attribute*.

Nel capitolo 5 viene descritta l'implementazione in Java. Tutto parte dalla definizione di uno *Status* e di conseguenza degli *Status Attribute*. Successivamente sono state implementate le funzioni per la modifica di questi attributi in modo da garantirne la mutabilità durante l'esecuzione delle richieste. Dopo sono state estese le *Obligations* in modo che potessero eseguire questo tipo di funzioni. L'ultimo passo invece è stato modificare il PEP in modo tale che potesse effettuare il *discharge* di questo nuovo tipo di *Obligations*.

6.1 FUTURO DI FAPCL

BIBLIOGRAFIA

- [1] NIST - *A survey of access Control Models* - http://csrc.nist.gov/news_events/privilege-management-workshop/PvM-Model-Survey-Aug26-2009.pdf (Cited on page 11.)
- [2] Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori - *Usage control in computer security: A Survey* (Cited on pages 17 and 71.)
- [3] Aliaksandr Lazouski, Gaetano Mancini, Fabio Martinelli, Paolo Mori - *Usage Control in Cloud Systems* - Istituto di informatica e Telematica, Consiglio Nazionale delle Ricerche. (Cited on page 17.)
- [4] FACPL Site - http://facpl.sourceforge.net/guide/facpl_guide.html
- [5] Jaehong Park, Ravi Sandhu - *The UCON Usage Control Model* - http://drjae.com/Publications_files/ucon-abc.pdf (Cited on page 9.)
- [6] Andrea Margheri, Massimiliano Masi, Rosario Pugliese, Francesco Tiezzi - *A Formal Framework for Specification, Analysis and Enforcement of Access Control Policies* (Cited on page 27.)
- [7] Jaehong Park, Ravi Sandhu - *Towards usage control models: beyond traditional access control*
- [8] Jaehong Park - *Usage control: A unified framework for next generation access control* - Tesi di dottorato, George Mason University
- [9] Eric Chabrow - *NIST Guide Aims to Ease Access Control* - <http://www.bankinfosecurity.com/nist-publication-aims-to-ease-access-control-a-6612/op-1>
- [10] Wikipedia, Access Control List - https://en.wikipedia.org/wiki/Access_control_list
- [11] Wikipedia, Role-based access control - https://en.wikipedia.org/wiki/Role-based_access_control

- [12] Wikipedia, Attribute-based access control - https://en.wikipedia.org/wiki/Attribute-based_access_control
- [13] Java Platform, Standard Edition 8 API Specification - <https://docs.oracle.com/javase/8/docs/api/>
- [14] ISO/IEC 14977 - *Information technology - Syntactic metalanguage - Extended BNF*
- [15] Xtext Documentation - <https://eclipse.org/Xtext/documentation/>

LISTA DI ACRONIMI

ACL	Access Control List
ABAC	Attribute Based Access Control
PBAC	Policy Based Access Control
RBAC	Role Based Access Control
PDP	Policy Decision Point
PEP	Policy Enforcement Point
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language
FACPL	Formal Access Control Policy Language
ACS	Access Control Policy
AAS	Authoritative Attribute Source

CODICE COMPLETO

A.1 CAPITOLO 4

Codice A.1: Secondo Esempio Completo

```
PolicySet Negozio { deny- unless- permit
  target: equal ( "Bob" , name / id ) || ( "Alice, name/id" )
  policies:

  PolicySet Buy_Policy { deny- unless- permit
    target: equal("file1", file/id) && ("buy", action/id)
    policies:
      Rule alice_buy ( permit target: (
        equal ( action / id , "buy" ) &&
        equal ( name / id, "Alice" ))
        obl:
          [ permit M setString("accessTypeAlice", "BUY" ) ]
        )
      Rule bob_buy ( permit target: (
        equal ( action / id , "buy" ) &&
        equal ( name / id, "Alice" ))
        obl:
          [ permit M setString("accessTypeBob", "BUY" ) ]
        )
    }

  PolicySet NUMBER_Policy { deny- unless- permit
    target: equal("file1", file/id) && ("number", action/id)
    policies:
      Rule alice_buy ( permit target: (
        equal ( action / id , "number" ) &&
        equal ( name / id, "Alice" ))
```

```

    obl:
    [ permit M setString("accessTypeAlice", "NUMBER") ]
    [ permit M addStatus("aliceFileIviewNumber", 2) ]
  )
  Rule bob_buy ( permit target: (
    equal ( action / id , "number" ) &&
    equal ( name / id, "Alice"))
    obl:
    [ permit M setString("accessTypeBob", "NUMBER") ]
    [ permit M addStatus("bobFileIviewNumber", 2) ]
  )
}

PolicySet TIME_Policy { deny- unless- permit
  target: equal("fileI", file/id) && ("TIME", action/id)
  policies:
    Rule alice_buy ( permit target: (
      equal ( action / id , "time" ) &&
      equal ( name / id, "Alice"))
      obl:
      [ permit M setString("accessTypeAlice", "TIME") ]
      [ permit M
        sumDate("aliceFileIexpiration", "0000/00/00-48:00:00") ]
    )
    Rule bob_buy ( permit target: (
      equal ( action / id , "time" ) &&
      equal ( name / id, "Alice"))
      obl:
      [ permit M setString("accessTypeBob", "TIME") ]
      [ permit M
        sumDate("bobFileIexpiration", "0000/00/00-48:00:00") ]
    )
  }

PolicySet VIEW { deny- unless- permit
  target: equal("fileI", file/id) && ("view", action/id)
  policies:
    Rule buy ( permit target: (
      equal ( status / accessTypeBob , "BUY" ) &&
      equal ( status / accessTypeAlice, "BUY"))
    )
    Rule number_alice ( permit target: (
      equal ( status / accessTypeAlice, "NUMBER" ) &&

```



```

    equal ( name / id, "Alice") && greater-than( status /
      aliceFileIviewNumber, 0))
    obl:
    [ permit M subStatus("aliceFileIviewNumber", 1) ]
  )
  Rule number_bob ( permit target: (
    equal ( status / accessTypeBob, "NUMBER" ) &&
    equal ( name / id, "Bob") && greater-than( status /
      bobFileIviewNumber, 0))
    obl:
    [ permit M subStatus("bobFileIviewNumber", 1) ]
  )
  Rule time_alice ( permit target: (
    equal ( status / accessTypeAlice, "TIME" ) &&
    equal ( name / id, "Alice") && greater-than( status /
      aliceFileIexpiration, today))
  )
  Rule number_alice ( permit target: (
    equal ( status / accessTypeAlice, "TIME" ) &&
    equal ( name / id, "Bob") && greater-than( status /
      bobFileIexpiration, today))
  )
}

}
PAS {
  Combined Decision : false ;
  Extended Indeterminate : false ;
  Java Package : "example" ;
  Requests To Evaluate : Request1, Request2, Request3, Request4,
    Request5, Request6 ;
  pep: deny- biased
  pdp: deny- unless- permit
  status: [ (date aliceFileIexpiration = today), (date
    bobFileIexpiration = today),
    (int bobFileIviewNumber = 0), (int aliceFileIviewNumber = 0),
    (String accessTypeAlice = "no"), (String accessTypeBob = "no")]
}

```

A.2 CAPITOLO 5

A.2.1 *Status e Status Attribute*

Codice A.2: Stralcio della classe Status

```

1 public class FacplStatus {
    private List<StatusAttribute> attributeList;
3    private String statusID;
    public FacplStatus(String statusID) {
5        attributeList = new ArrayList<StatusAttribute>();
        this.statusID = statusID;
7    }
    public FacplStatus(List<StatusAttribute> attributeList, String
        statusID) {
9        this.attributeList = attributeList;
        this.statusID = statusID;
11    }
    public FacplStatus() {
13        attributeList = new ArrayList<StatusAttribute>();
        this.statusID = UUID.randomUUID().toString().substring(0, 8);
15    }
    public String getStatusID() {
17        return this.statusID;
    }
    public void add(StatusAttribute a) {
19        this.attributeList.add(a);
21    }
    public StatusAttribute retrieveAttribute(StatusAttribute
        attribute) throws MissingAttributeException {
23        int i = this.attributeList.indexOf(attribute);
        if (i != -1) {
25            return this.attributeList.get(i);
        } else {
27            throw new MissingAttributeException("attribute doesn't exist in the
                current status");
        }
29    }
    public Object getValue(StatusAttribute attribute) throws
        MissingAttributeException {
31        return (Object) (this.retrieveAttribute(attribute).getValue());
    }

```

33
}

Codice A.3: Costruttori di Status Attribute

```

public class StatusAttribute {
2   private String id;
   private FacplStatusType type;
4   private String value;
   public StatusAttribute(String id, FacplStatusType type) {
6       this.id = id;
       this.type = type;
8       if (type == (FacplStatusType.INT) || type ==
           (FacplStatusType.DOUBLE)) {
           value = "0";
10      } else if (type == FacplStatusType.BOOLEAN) {
           value = "false";
12      } else if (type == FacplStatusType.DATE) {
           value = "0";
14      } else {
           value = "";
16      }
   }
18   public StatusAttribute(String id, FacplStatusType type, String
       value) {
       this.id = id;
20      this.type = type;
       this.value = value;
22   }
   public String getValue() {
24       return value;
   }
26   public void setValue(String value) {
       this.value = value;
28   }
   public String getId() {
30       return id;
   }
32   public void setId(String id) {
       this.id = id;
34   }
   public FacplStatusType getType() {
36       return type;

```

```

    }
38 public void setType(FacplStatusType type) {
    this.type = type;
40 }
@Override
42 public boolean equals(Object obj) {
    if (obj instanceof StatusAttribute) {
44         StatusAttribute o = (StatusAttribute) obj;
        return this.getId() == o.getId() && this.getType() ==
            o.getType();
46     }
    return false;
48 }
@Override
50 public String toString() {
    return this.type.toString() + "/" + this.id + "/" +
        this.value.toString();
52 }
54 }

```

A.2.2 Implementazione dei comparatori sugli Status Attribute

Codice A.4: Classe che implementa Equal

```

public class Equal implements IComparisonFunction {
2 public Boolean evaluateFunction(List<Object> args) throws
    Throwable {
    if (args.size() == 2) {
4        Object o1, o2;
        o1 = args.get(0) instanceof StatusAttribute ?
            this.convertType((StatusAttribute) args.get(0)) :
            args.get(0);
6        o2 = args.get(1) instanceof StatusAttribute ?
            this.convertType((StatusAttribute) args.get(1)) :
            args.get(1);
        IComparisonEvaluator evaluator =
            ComparisonEvaluatorFactory.getInstance().getEvaluator(o1);
8        return evaluator.areEquals(o1, o2);
    } else {
10        throw new Exception("Illegal number of arguments");
    }
}

```

```

    }
12 }
    private Object convertType(StatusAttribute sa) {
14     if (sa.getType() == FacplStatusType.BOOLEAN) {
        if (sa.getValue() == "true") {
16             return true;
        } else
18             return false;
    } else if (sa.getType() == FacplStatusType.DOUBLE) {
20         return (Double)Double.parseDouble(sa.getValue());
    } else if (sa.getType() == FacplStatusType.INT) {
22         return (Integer)Integer.parseInt(sa.getValue());
    } else if (sa.getType() == FacplStatusType.STRING) {
24         return sa.getValue();
    }
26     return null;
    }
28 }

```

A.2.3 Funzioni per la modifica degli Status Attribute

Codice A.5: Metodo implementato dall'interfaccia

```

package it.unifi.facpl.system.status.function.arithmetic.evaluator;

2
import java.util.Calendar;

4
import it.unifi.facpl.lib.enums.FacplStatusType;
6 import it.unifi.facpl.lib.function.comparison.evaluator.Util;
import it.unifi.facpl.lib.util.FacplDate;
8 import it.unifi.facpl.lib.util.exception.UnsupportedTypeException;
import it.unifi.facpl.system.status.StatusAttribute;

10
public class NumberArithmeticEvaluatorStatus implements
    ArithmeticEvaluatorStatus {

12
    private static NumberArithmeticEvaluatorStatus instance;

14
    private NumberArithmeticEvaluatorStatus() {

16
    }

```

```

18     public static NumberArithmeticEvaluatorStatus getInstance() {
20         if (instance == null) {
21             instance = new NumberArithmeticEvaluatorStatus();
22         }
23         return instance;
24     }

26     @Override
27     public void add(StatusAttribute o1, Object o2) throws Throwable {
28         if (o1.getType() == FacplStatusType.INT) {
29             Integer value = Integer.parseInt(o1.getValue());
30             Integer newValue = value + (int) o2;
31             o1.setValue(newValue.toString());
32         } else if (o1.getType() == FacplStatusType.DOUBLE) {
33             Double value = Double.parseDouble(o1.getValue());
34             Double newValue = value + (double) o2;
35             o1.setValue(newValue.toString());
36         } else {
37             throw new UnsupportedOperationException("Number", "Add");
38         }
39     }

40     @Override
41     public void divide(StatusAttribute o1, Object o2) throws
42         Throwable {
43         if (o1.getType() == FacplStatusType.INT) {
44             Integer value = Integer.parseInt(o1.getValue());
45             Integer newValue = value / (int) o2;
46             o1.setValue(newValue.toString());
47         } else if (o1.getType() == FacplStatusType.DOUBLE) {
48             Double value = Double.parseDouble(o1.getValue());
49             Double newValue = value / (double) o2;
50             o1.setValue(newValue.toString());
51         } else {
52             throw new UnsupportedOperationException("Number", "div");
53         }
54     }

56     @Override
57     public void multiply(StatusAttribute o1, Object o2) throws
58         Throwable {

```

```

58     if (o1.getType() == FacplStatusType.INT) {
        Integer value = Integer.parseInt(o1.getValue());
60     Integer newValue = value * (int) o2;
        o1.setValue(newValue.toString());
62     } else if (o1.getType() == FacplStatusType.DOUBLE) {
        Double value = Double.parseDouble(o1.getValue());
64     Double newValue = value * (double) o2;
        o1.setValue(newValue.toString());
66     } else {
        throw new UnsupportedOperationException("Number", "mul");
68     }
    }

70
@Override
72 public void subtract(StatusAttribute o1, Object o2) throws
    Throwable {
    if (o1.getType() == FacplStatusType.INT) {
74     Integer value = Integer.parseInt(o1.getValue());
        Integer newValue = value - (int) o2;
76     o1.setValue(newValue.toString());
    } else if (o1.getType() == FacplStatusType.DOUBLE) {
78     Double value = Double.parseDouble(o1.getValue());
        Double newValue = value - (double) o2;
80     o1.setValue(newValue.toString());
    } else {
82     throw new UnsupportedOperationException("Number", "sub");
    }
84 }

86
@Override
public void flag(StatusAttribute o1, Object o2) throws Throwable {
88     if (o1.getType() == FacplStatusType.BOOLEAN && o2 instanceof
        Boolean) {
        Boolean newValue = (Boolean) o2;
90     o1.setValue(newValue.toString());

92     } else {
        throw new UnsupportedOperationException("Boolean", "Flag");
94     }

96 }

```

```

98  @Override
    public void sum_date(StatusAttribute o1, Object o2) throws
        Throwable {
100     if (o1.getType() == FacplStatusType.DATE) {
        Calendar d1 = Util.parseDate(o1.getValue());
102     Calendar d2 = Util.parseDate(((FacplDate) o2).toString());
        d1.add(d1.HOUR, d2.get(d2.HOUR));
104     d1.add(d1.MINUTE, d2.get(d2.MINUTE));
        d1.add(d1.SECOND, d2.get(d2.SECOND));
106     o1.setValue(Util.parseCalendar(d1));
    } else {
108     throw new UnsupportedOperationException("Date", "Add");
    }
110 }
112 }

```

A.2.4 *Obligations e PEP*

Codice A.6: Parte rifattorizzata del metodo che si occupa del fulfilling

```

1  public abstract class AbstractObligation implements
    IObligationElement {
        protected Effect evaluatedOn;
3   protected ObligationType typeObl;
        protected Object pepAction;
5   protected LinkedList<Object> argsFunction, argsStatus;
        public AbstractObligation(Effect evaluatedOn, ObligationType
            type, Object... args) {
7       this.evaluatedOn = evaluatedOn;
            this.typeObl = type;
9       this.argsFunction = new LinkedList<Object>();
            this.argsStatus = new LinkedList<Object>();
11    }
        protected abstract AbstractFulfilledObligation createObligation();
13    @Override
        public AbstractFulfilledObligation
            getObligationValue(ContextRequest cxtRequest) throws
                FulfillmentFailed {
15        Logger l = LoggerFactory.getLogger(Obligation.class);

```



```

    l.debug("Fulfilling Obligation " + this.pepAction.toString() + "...");
17 AbstractFulfilledObligation obl = this.createObligation();
    if (obl instanceof FulfilledObligationCheck) {
19         l.debug("...created FulfilledObligationCHECK: " + obl.toString());
        return obl;
21     }
    for (Object arg : argsFunction) {
23         if (arg instanceof ExpressionFunction) {
            Object res = ((ExpressionFunction)
                arg).evaluateExpression(cxtRequest);
25             if (res.equals(ExpressionValue.BOTTOM) ||
                res.equals(ExpressionValue.ERROR)) {
                throw new FulfillmentFailed();
27             }
            obl.addArg(res);
29         } else if (arg instanceof ExpressionBooleanTree) {
            ExpressionValue res = ((ExpressionBooleanTree)
                arg).evaluateExpressionTree(cxtRequest);
31             if (res.equals(ExpressionValue.BOTTOM) ||
                res.equals(ExpressionValue.ERROR)) {
                throw new FulfillmentFailed();
33             }
            obl.addArg(res);
35         } else if (arg instanceof AttributeName) {
            try {
37                 obl.addArg(cxtRequest.getContextRequestValues((AttributeName)
                    arg));
            } catch (MissingAttributeException e) {
39                 throw new FulfillmentFailed();
            }
41         } else {
            obl.addArg(arg);
43         }
    }
45     l.debug("...fulfillment completed. Arguments: " +
        obl.getArguments().toString());
    return obl;
47 }

49 @Override
    public Effect getEvaluatedOn() {
51         return this.evaluatedOn;

```

```

    }
53  @Override
    public ObligationType getTypeObl() {
55      return this.typeObl;
    }
57 }

```

Codice A.7: CreateObligation nelle status

```

1  public class ObligationStatus extends AbstractObligation {
    public ObligationStatus(IEExpressionFunctionStatus pepAction,
        Effect evaluatedOn, ObligationType type,
3      Object... args) {
        super(evaluatedOn, type, args);
5      this.pepAction = pepAction;
        if (args != null) {
7          for (Object ob : args) {
                if (ob instanceof StatusAttribute || ob instanceof Integer
                    || ob instanceof Double
9                || ob instanceof Boolean || ob instanceof FacplDate) {
                    argsStatus.add(ob);
11                }
                argsFunction.add(ob);
13            }
        }
15    }
    @Override
17    protected AbstractFulfilledObligation createObligation() {
        AbstractFulfilledObligation obl = new
            FulfilledObligationStatus(this.evaluatedOn, this.typeObl,
19            (IEExpressionFunctionStatus) this.pepAction);
        if (!argsStatus.isEmpty()) {
21            obl.addArgStatus(argsStatus);
        }
23        return obl;
    }
25 }

```

Codice A.8: CreateObligation nelle normali

```

1  public class Obligation extends AbstractObligation {
    public Obligation(String pepAction, Effect evaluatedOn,
        ObligationType type, Object... args) {

```

```

3      super(evaluatedOn, type, args);
      this.pepAction = pepAction;
5      if (args != null) {
          for (Object ob : args) {
7              argsFunction.add(ob);
          }
9      }
      }
11  @Override
      protected AbstractFulfilledObligation createObligation() {
13      return new FullfilledObbligation(this.evaluatedOn,
          this.typeObl, (String) this.pepAction);
      }
15 }

```

Codice A.9: Discharge delle Fulfilled Obligation di stato

```

1  public class PEP {
      private static HashMap<String, Class<? extends IPepAction>>
          pepAction;
3      private EnforcementAlgorithm alg;
      public PEP(EnforcementAlgorithm alg) {
5          this.alg = alg;
      }
7      public AuthorisationPEP doEnforcement(AuthorisationPDP authPDP) {
          Logger l = LoggerFactory.getLogger(PEP.class);
9          l.debug("Start PEP enforcement for request: " + authPDP.getId());
          l.debug("Authorisation to enforce: " + authPDP.toString());
11
          if (pepAction == null) {
13              l.debug("Pep actions not initialized");
          }
15          try {
              AuthorisationPEP decPEP = null;
17              StandardDecision dec = authPDP.getStandardDecision();
              switch (this.alg) {
19                  case BASE:
                      l.debug("Chosen Enforcement Algorithm " + alg.toString());
21                      if (dec.equals(StandardDecision.DENY) ||
                          dec.equals(StandardDecision.PERMIT)) {
                          for (AbstractFulfilledObligation obl :
                              authPDP.getObligation()) {
23                          try {

```

```

        this.dischargeObligation(obl);
25     } catch (Throwable t) {
        l.debug("Obligation Evaluation Failed");
27     l.debug("Enforced Decision:" +
            StandardDecision.INDETERMINATE);
        return new AuthorisationPEP(authPDP.getId(),
            StandardDecision.INDETERMINATE);
29     }
    }
31    decPEP = new AuthorisationPEP(authPDP.getId(), dec);
} else {
33    l.debug("No Obligations to discharge. Enforcement
        completed");
    decPEP = new AuthorisationPEP(authPDP.getId(), dec);
35 }
break;
37 case DENY_BIASED:
    l.debug("Chosen Enforcement Algorithm " + alg.toString());
39    if (dec.equals(StandardDecision.PERMIT)) {
        for (AbstractFulfilledObligation obl :
            authPDP.getObligation()) {
41            try {
                this.dischargeObligation(obl);
43            } catch (Throwable t) {
                l.debug("Obligation Evaluation Failed");
45                l.debug("Enforced Decision:" + StandardDecision.DENY);
                return new AuthorisationPEP(authPDP.getId(),
                    StandardDecision.DENY);
47            }
        }
49        decPEP = new AuthorisationPEP(authPDP.getId(), dec);
    } else {
51        l.debug("No Obligations to discharge. Enforcement
            completed");
        decPEP = new AuthorisationPEP(authPDP.getId(),
            StandardDecision.DENY);
53    }
    break;
55 case PERMIT_BIASED:
    if (dec.equals(StandardDecision.DENY)) {
57        for (AbstractFulfilledObligation obl :
            authPDP.getObligation()) {

```

```

        try {
59             this.dischargeObligation(obl);
        } catch (Throwable t) {
61             l.debug("Obligations Evaluation Failed");
            l.debug("Enforced Decision:" +
                StandardDecision.PERMIT);
63             return new AuthorisationPEP(authPDP.getId(),
                StandardDecision.PERMIT);
        }
65     }
    decPEP = new AuthorisationPEP(authPDP.getId(), dec);
67 } else {
    l.debug("No Obligations to discharge. Enforcement
        completed");
69     decPEP = new AuthorisationPEP(authPDP.getId(),
        StandardDecision.PERMIT);
    }
71     break;
}
73     l.debug("Enforced Decision:" + decPEP.toString());
    return decPEP;
75 } catch (Throwable t) {
    l.debug("Unhandled Exception. Enforced Decision:
        INDETERMINATE");
77     return new AuthorisationPEP(authPDP.getId(),
        StandardDecision.INDETERMINATE);
    }
79 }
private void dischargeObligation(AbstractFulfilledObligation obl)
    throws Throwable {
81     Logger l = LoggerFactory.getLogger(PEP.class);
    if (obl instanceof FullfilledObbligation) {
83         obl = (FullfilledObbligation) obl;
        try {
85             Class<? extends IPepAction> classAction =
                pepAction.get((String) obl.getPepAction());
            if (classAction == null) {
87                 l.debug("Undefined PEP action \"" + (String)
                    obl.getPepAction() + "\"");
                throw new Exception("Undefined " + (String)
                    obl.getPepAction() + " PEP Action");
89             }

```

```

        Class<?> params[] = new Class[1];
91     params[0] = List.class;
        Method eval = classAction.getDeclaredMethod("eval", params);
93     Object pepAction = classAction.newInstance();
        eval.invoke(pepAction, obl.getArguments());
95     } catch (Throwable t) {
        if (obl.getType().equals(ObligationType.M)) {
97         throw t;
        }
99     l.debug("Exception ignored. Obligation is optional");
    }
101 }
    else if (obl instanceof FulfilledObligationStatus) {
103     obl = (FulfilledObligationStatus) obl;
        obl.evaluateObl();
105     }
    }
107 }
    public void addPEPActions(HashMap<String, Class<? extends
        IPepAction>> classPepActions) {
109     Logger l = LoggerFactory.getLogger(PEP.class);
        l.debug("Add standard actions");
111
        pepAction = new HashMap<String, Class<? extends IPepAction>>();
113     pepAction.put("mail",
        it.unifi.facpl.lib.pepFunction.MailTo.class);
        pepAction.put("log", it.unifi.facpl.lib.pepFunction.Log.class);
115     pepAction.put("compress",
        it.unifi.facpl.lib.pepFunction.Compress.class);

117     if (classPepActions != null) {
        for (String key : classPepActions.keySet()) {
119         l.debug("Add action " + key);
        }
121     pepAction.putAll(classPepActions);
    }
123 }
125 }
}

```

A.2.5 Esempio

Codice A.10: Policy StopRead

```

public class PolicySet_ReadWrite extends PolicySet {
2   protected ContextRequest_Status ctxReq;
   public PolicySet_ReadWrite(ContextRequest_Status ctxReq) throws
       MissingAttributeException {
4       this.ctxReq = ctxReq;
       addId("ReadWrite_Policy");
6       addCombiningAlg(it.unifi.facpl.lib.algorithm.DenyUnlessPermitGreedy.class);
       ExpressionFunction e1 = new
           ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
               "Bob",
8           new AttributeName("name", "id"));
       ExpressionFunction e2 = new
           ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
               "Alice",
10          new AttributeName("name", "id"));
       ExpressionBooleanTree ebt = new
           ExpressionBooleanTree(ExprBooleanConnector.OR, e1, e2);
12      addTarget(ebt);
       addPolicyElement(new PolicySet_Write(ctxReq));
14      addPolicyElement(new PolicySet_Read(ctxReq));
       addPolicyElement(new PolicySet_StopWrite(ctxReq));
16      addPolicyElement(new PolicySet_StopRead(ctxReq));
   }
18  private class PolicySet_Write extends PolicySet {
       protected ContextRequest_Status ctxReq;
20      public PolicySet_Write(ContextRequest_Status ctxReq) throws
          MissingAttributeException {
           this.ctxReq = ctxReq;
22          addId("Write_Policy");
           addCombiningAlg(it.unifi.facpl.lib.algorithm.DenyUnlessPermitGreedy.class);
24          ExpressionFunction e1 = new
              ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                  "file1",
26                  new AttributeName("file", "id")
              );
28          ExpressionFunction e2 = new
              ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                  "write",

```

```

30         new AttributeName("action", "id")
           );
32     ExpressionBooleanTree ebt = new
        ExpressionBooleanTree(ExprBooleanConnector.AND, e1, e2);
    addTarget(ebt);
34     addPolicyElement(new Rule_write());
    addObligation(new ObligationStatus(new FlagStatus(),
        Effect.PERMIT, ObligationType.M,
36         ctxReq.getStatusAttribute(new
            StatusAttribute("isWriting",
                FacplStatusType.BOOLEAN)), true));
    }
38     private class Rule_write extends Rule {
        Rule_write() throws MissingAttributeException {
40             addId("write");
            addEffect(Effect.PERMIT);
42             ExpressionFunction e1=new
                ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                    ctxReq.getStatusAttribute(
44                        ctxReq.getStatusAttribute(new
                            StatusAttribute("isWriting",
                                FacplStatusType.BOOLEAN))),
                        false);
46             ExpressionFunction e2=new
                ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                    ctxReq.getStatusAttribute(
48                        ctxReq.getStatusAttribute(new
                            StatusAttribute("counterReadFile1",
                                FacplStatusType.INT))),
                        0);
50             ExpressionBooleanTree ebt = new
                ExpressionBooleanTree(ExprBooleanConnector.AND, e1, e2);
            addTarget(ebt);
52         }
    }
54 }

56     private class PolicySet_Read extends PolicySet {
        protected ContextRequest_Status ctxReq;
        public PolicySet_Read(ContextRequest_Status ctxReq) throws
            MissingAttributeException {
58             this.ctxReq = ctxReq;
            addId("Read_Policy");

```



```

60     addCombiningAlg(it.unifi.facpl.lib.algorithm.DenyUnlessPermitGreedy.class);
    ExpressionFunction e1 = new
        ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
62         "file1",
        new AttributeName("file", "id")
64         );
    ExpressionFunction e2 = new
        ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
66         "read",
        new AttributeName("action", "id")
68         );
    ExpressionBooleanTree ebt = new
        ExpressionBooleanTree(ExprBooleanConnector.AND, e1, e2);
70     addTarget(ebt);
    addPolicyElement(new Rule_read());
72     addObligation(new ObligationStatus(new AddStatus(),
        Effect.PERMIT, ObligationType.M,
        ctxReq.getStatusAttribute(new
            StatusAttribute("counterReadFile1",
            FacplStatusType.INT)), 1));
74 }
private class Rule_read extends Rule {
76     Rule_read() throws MissingAttributeException {
        addId("read");
78         addEffect(Effect.PERMIT);
        ExpressionFunction e1 = new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
80             ctxReq.getStatusAttribute(
                ctxReq.getStatusAttribute(new
                    StatusAttribute("isWriting",
                    FacplStatusType.BOOLEAN))),
82             false);
        ExpressionFunction e2 = new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.LessThan.class,
84             ctxReq.getStatusAttribute(
                ctxReq.getStatusAttribute(new
                    StatusAttribute("counterReadFile1",
                    FacplStatusType.INT))),
86             2);
        ExpressionBooleanTree ebt = new
            ExpressionBooleanTree(ExprBooleanConnector.AND, e1, e2);
88         addTarget(ebt);

```

```

    }
90 }
}
92 private class PolicySet_StopRead extends PolicySet {
    protected ContextRequest_Status ctxReq;
94 public PolicySet_StopRead(ContextRequest_Status ctxReq) throws
        MissingAttributeException {
        this.ctxReq = ctxReq;
96 addId("StopRead_Policy");
        addCombiningAlg(it.unifi.facpl.lib.algorithm.DenyUnlessPermitGreedy.class);
98 ExpressionFunction e1 = new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                "file1",
100         new AttributeName("file", "id")
            );
102 ExpressionFunction e2 = new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                "stopRead",
104         new AttributeName("action", "id")
            );
106 ExpressionBooleanTree ebt = new
            ExpressionBooleanTree(ExprBooleanConnector.AND, e1, e2);
        addTarget(ebt);
108 addPolicyElement(new Rule_stopRead());
        addObligation(new ObligationStatus(new SubStatus(),
            Effect.PERMIT, ObligationType.M,
110         ctxReq.getStatusAttribute(new
            StatusAttribute("counterReadFile1",
                FacplStatusType.INT)), 1));
    }
112 private class Rule_stopRead extends Rule {
        Rule_stopRead() throws MissingAttributeException {
114         addId("stopRead");
            addEffect(Effect.PERMIT);
116         addTarget(new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.GreaterThan.class,
                ctxReq.getStatusAttribute(
118         ctxReq.getStatusAttribute(new
            StatusAttribute("counterReadFile1",
                FacplStatusType.INT))),
                0));
120     }

```

```

    }
122 }

124 private class PolicySet_StopWrite extends PolicySet {
    protected ContextRequest_Status ctxReq;
126 public PolicySet_StopWrite(ContextRequest_Status ctxReq) throws
        MissingAttributeException {
        this.ctxReq = ctxReq;
128 addId("StopWrite_Policy");
        addCombiningAlg(it.unifi.facpl.lib.algorithm.DenyUnlessPermitGreedy.class);
130 ExpressionFunction e1 = new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                "file1",
132         new AttributeName("file", "id")
            );
134 ExpressionFunction e2 = new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                "stopWrite",
136         new AttributeName("action", "id")
            );
138 ExpressionBooleanTree ebt = new
            ExpressionBooleanTree(ExprBooleanConnector.AND, e1, e2);
        addTarget(ebt);
140 addPolicyElement(new Rule_write());
        addObligation(new ObligationStatus(new FlagStatus(),
            Effect.PERMIT, ObligationType.M,
142         ctxReq.getStatusAttribute(new
            StatusAttribute("isWriting",
                FacplStatusType.BOOLEAN)), false));
    }
144 private class Rule_write extends Rule {
        Rule_write() throws MissingAttributeException {
146         addId("stopWrite");
            addEffect(Effect.PERMIT);
148         addTarget(new
            ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
                ctxReq.getStatusAttribute(
150         ctxReq.getStatusAttribute(new
            StatusAttribute("isWriting",
                FacplStatusType.BOOLEAN))),
            true));
152     }

```

```

    }
154 }
}

```

Codice A.11: Policy StopRead

```

1  private class PolicySet_StopRead extends PolicySet {
    protected ContextRequest_Status ctxReq;
3  public PolicySet_StopRead(ContextRequest_Status ctxReq) throws
    MissingAttributeException {
    this.ctxReq = ctxReq;
5  addId("StopRead_Policy");
    addCombiningAlg(it.unifi.facpl.lib.algorithm.DenyUnlessPermitGreedy.class);
7  ExpressionFunction e1 = new
    ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
        "file1",
9      new AttributeName("file", "id")
        );
11  ExpressionFunction e2 = new
    ExpressionFunction(it.unifi.facpl.lib.function.comparison.Equal.class,
        "stopRead",
13     new AttributeName("action", "id")
        );
15  ExpressionBooleanTree ebt = new
    ExpressionBooleanTree(ExprBooleanConnector.AND, e1, e2);
    addTarget(ebt);
17  addPolicyElement(new Rule_stopRead());
    addObligation(new ObligationStatus(new SubStatus(),
        Effect.PERMIT, ObligationType.M,
19     ctxReq.getStatusAttribute(new
        StatusAttribute("counterReadFile1",
            FacplStatusType.INT)), 1));
    }
21 private class Rule_stopRead extends Rule {
    Rule_stopRead() throws MissingAttributeException {
23     addId("stopRead");
    addEffect(Effect.PERMIT);
25     addTarget(new
        ExpressionFunction(it.unifi.facpl.lib.function.comparison.GreaterThan.class,
            ctxReq.getStatusAttribute(
27         ctxReq.getStatusAttribute(new
            StatusAttribute("counterReadFile1",
                FacplStatusType.INT))),

```

```

                                0));
29         }
        }
31     }
```
