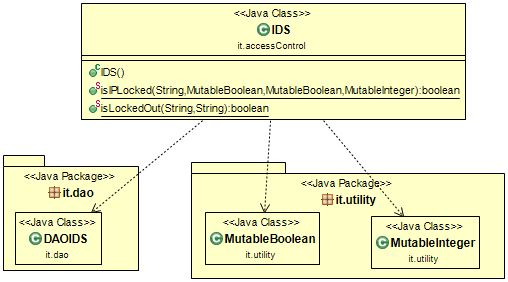
Diagramma delle classi

Di seguito viene riportato il diagramma delle classi di WebRTC\_Secure: piuttosto che limitarci ad allegare un solo diagramma, troppo complesso e poco informativo, si riportano le classi per package e relazioni intra ed inter-package; in questo modo abbiamo suddiviso il diagramma delle classi originali in porzioni sufficientemente piccole da poter essere analizzate con profitto ma sufficientemente grandi da essere significative, che nell’insieme permette ad un programmatore la giusta documentazione per individuare struttura e dipendenza delle classi con l’adeguata granularità di informazioni.

Per ragioni di semplicità sono state omesse le relazioni al package delle eccezioni, da cui praticamente tutti i package dipendono.

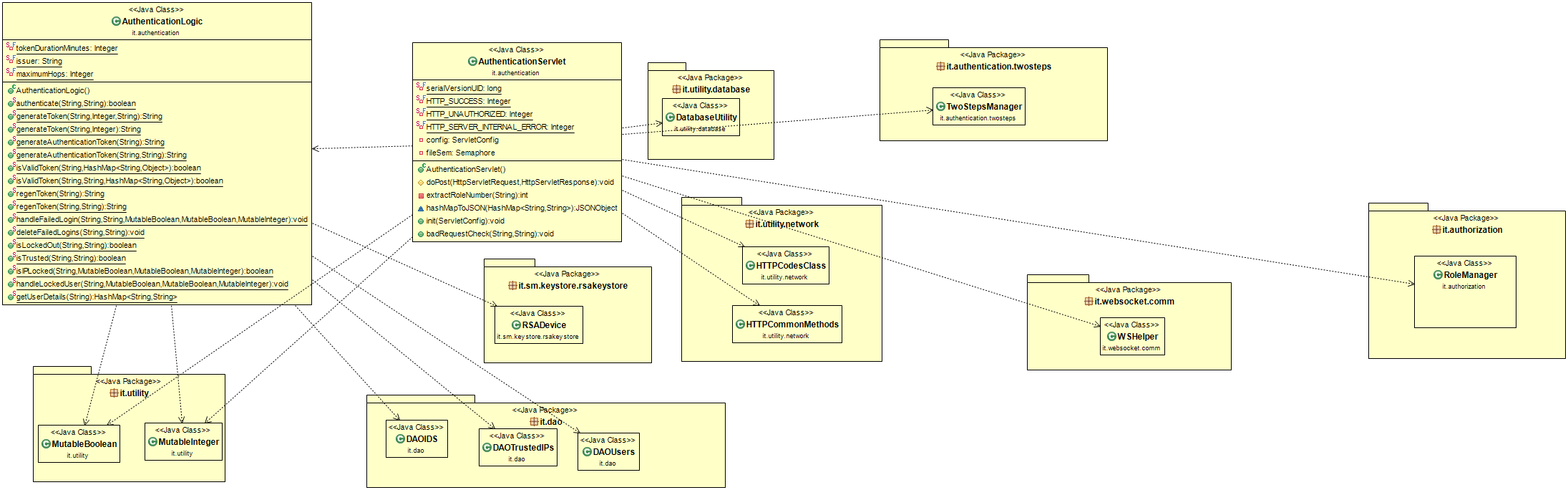
Package Access Control

Contiene la classe che si occupa delle operazioni per prevenire o individuare le intrusioni in un account, aggiornare i conteggi dei login falliti e bloccare i tentativi di accesso.

****

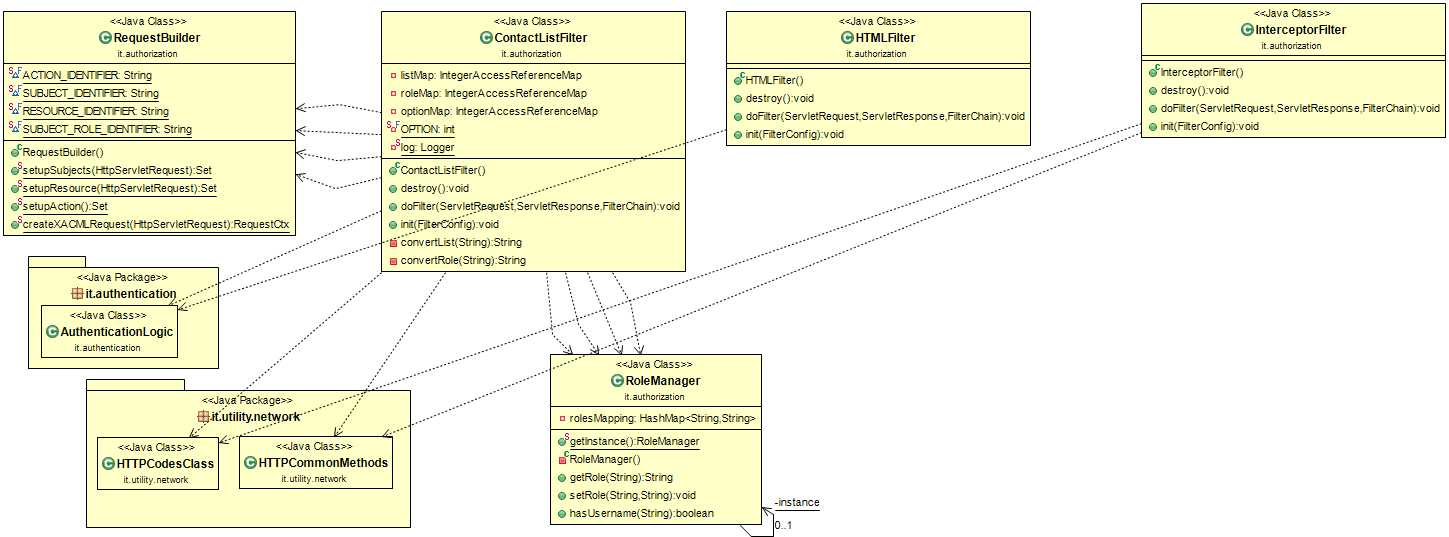
Package authentication

Appartengono a questo package la servlet di autenticazione e la relativa logica (disaccoppiata dalla servlet per il principio della separazione degli interessi)



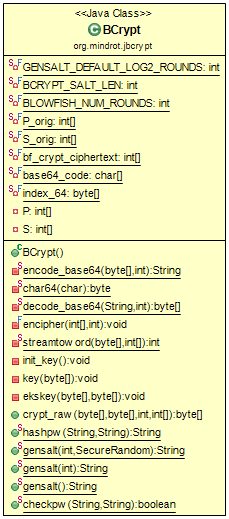
Package authorization

Le classi di questo package si occupano di determinare se l’utente è autorizzato ad effettuare una determinata operazione.



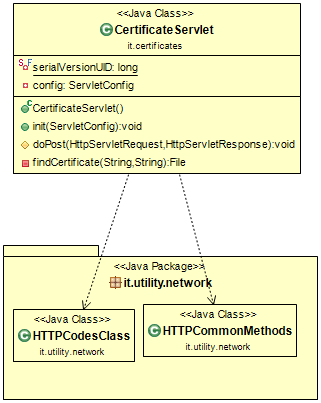
Package bcrypt

Package importato da una libreria OTS che implementa hashing/salting delle password con algoritmo bcrypt (utilizzato, fra gli altri, da OpenBSD)



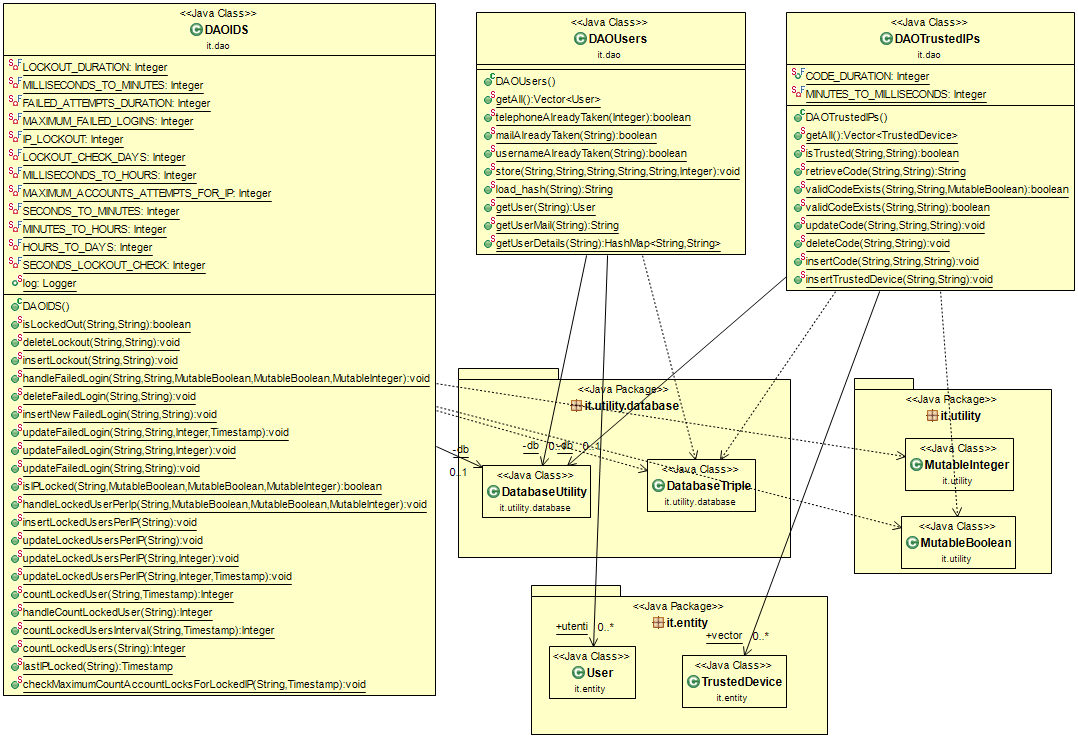
Package Certificates

Contiene la servlet a cui rivolgersi per recuperare i certificati associati ad utenti, tecnici ed amministratori.



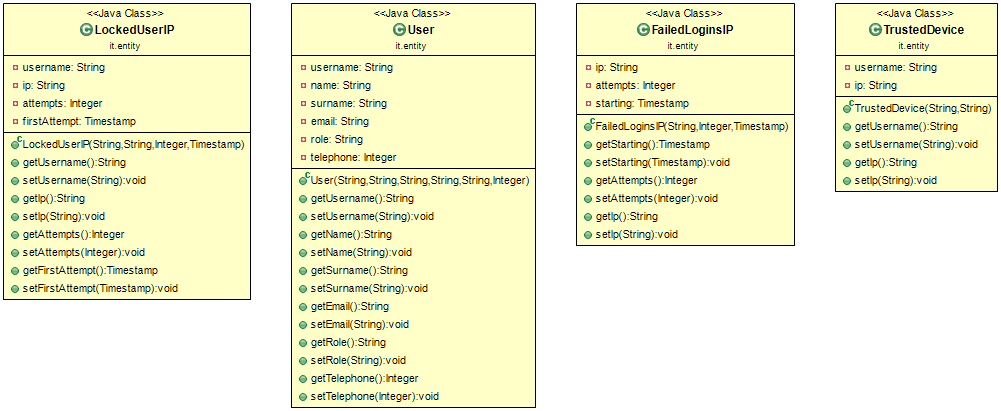
Package dao

Questo package rappresenta il ponte tra i dati del db e l’applicazione. Sono le classi a cui le altre si rivolgono per operare su dati che altrimenti sarebbero da prelevare direttamente dal database.



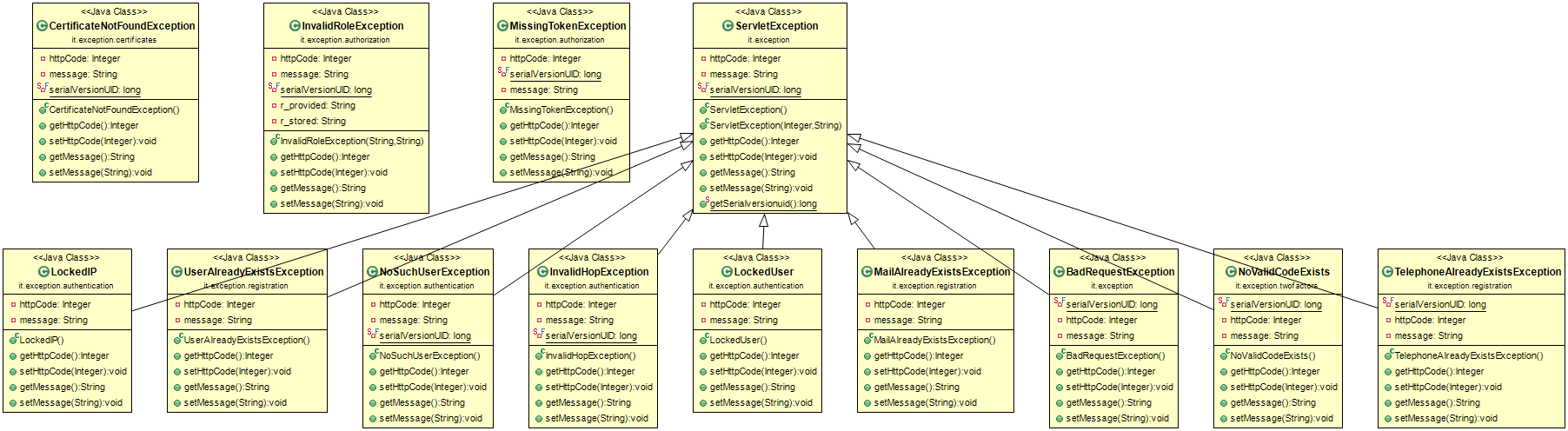
Package entity

Costituiscono una rappresentazione Object-oriented che effettua il mapping rispetto alla rappresentazione del db.



Package exception

Raccoglie tutte le eccezioni che possono essere lanciate. A sua volta è diviso in sotto-package che non vengono rappresentati per semplicità.



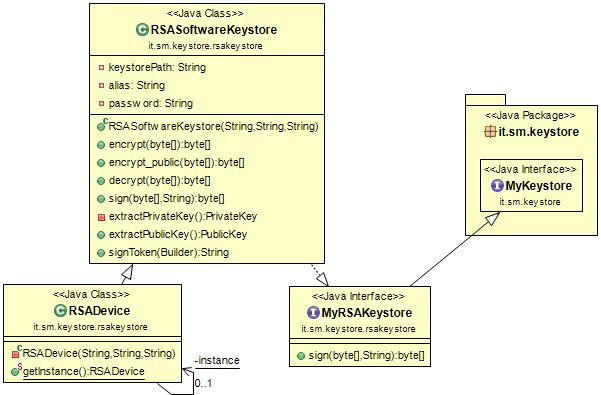
Package keystore

Contiene la semplice interfaccia che ci aspetteremmo da un’entità crittografica: la capacità di criptare e decriptare bytes. Implementeranno l’interfaccia tutte quelle classi che si occuperanno di crittografare dati (implementando gli specifici algoritmi di cui MyKeystore è indipendente)



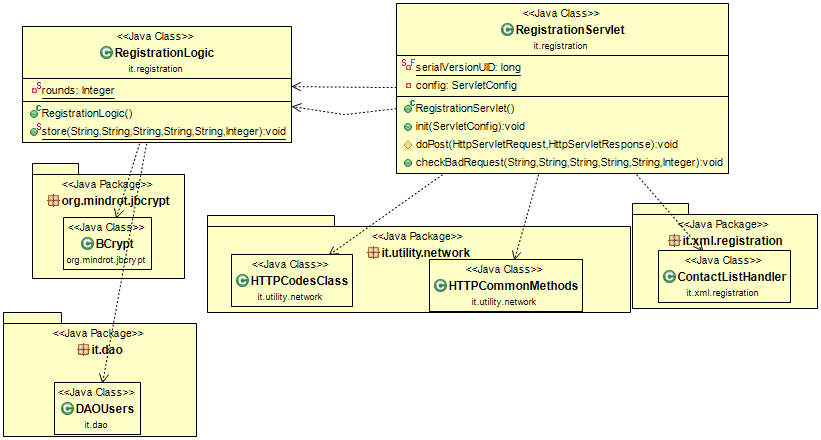
Package keystore.rsaKeystore

Package innestato nel precedente che rappresenta una crittografia specifica, in questo caso di tipo RSA. Simula le caratteristiche di una smart-card (di cui avremmo bisogno per una criptografia sicura) in software, e usa le chiavi private e pubblica per codificare e decodificare: la privata viene usate per codificare i dati da mandare al client, la pubblica quelli che solo il server può leggere, come la chiave AES utilizzata per codificare i parametri di accesso al db e al mail server.



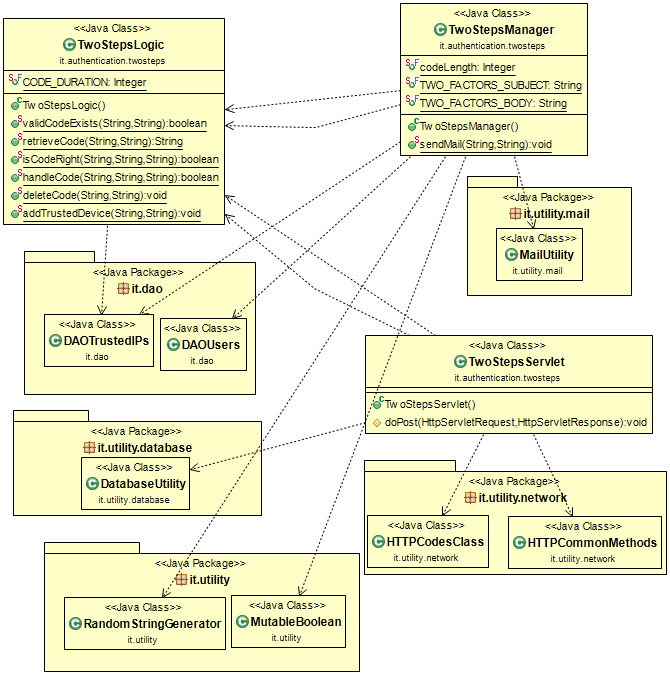
Package registration

Appartengono a questo package la servlet e la logica di registrazione.



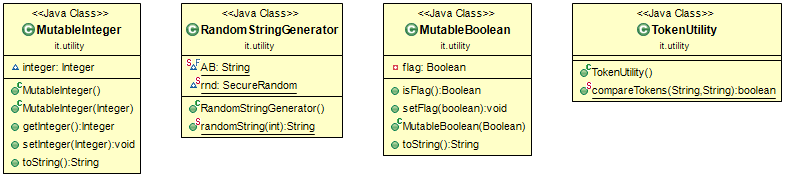
Package twosteps

Di questo package fanno parte le classi che si occupano dell’autenticazione in due passi; la classe TwoStepsServlet rappresenta la servlet a cui rivolgersi per l’invio del codice, ed effettua chiamate a TwoStepsLogic per ciò che concerne la logica delle operazioni, mentre TwoStepsManager si occupa dell’invio della mail nel caso in cui fosse richiesta



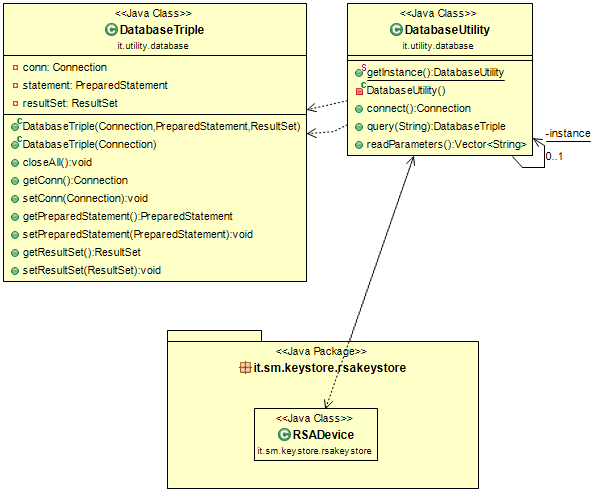
Package utility

Contiene diverse classi di utilità, utilizzate per risolvere in modo semplice alcuni task, come la generazione del codice per l’autenticazione a due step (RandomStringGenerator).



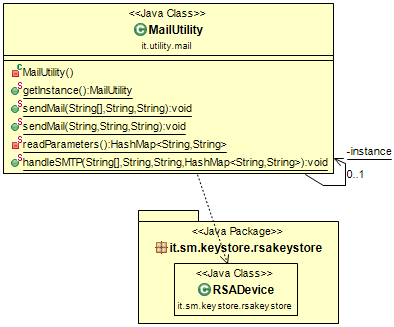
Package utility.database

A questo package appartengono delle classi di utilità create per rendere più semplice alcune operazioni di routine sul database.



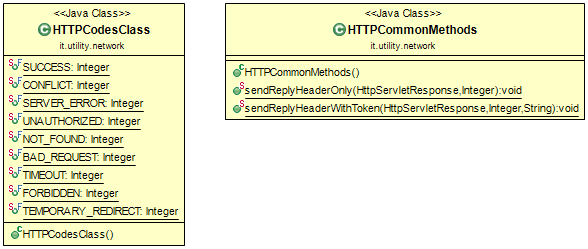
Package utility.mail

Contiene la classe per l’interfacciamento al mail server.



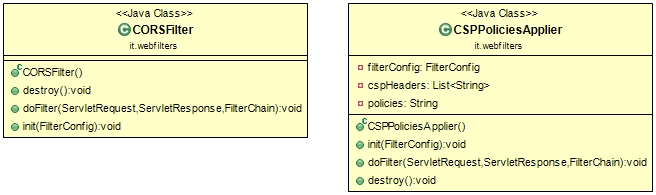
Package utility.network

Contiene delle classi di utilità utilizzate per inviare risposte http e altre operazioni di routine.



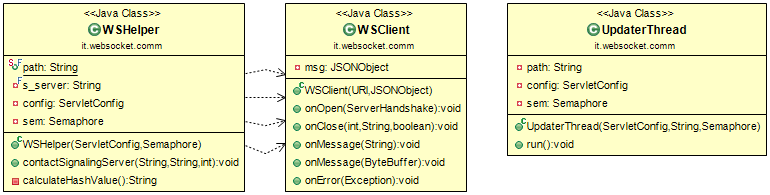
Package webfilter

Le classi di questo package risolvono diversi problemi come il Cross Origin Resource Sharing



Package websocket

Questo package contiene le classi per la gestione delle Web Socket.



Package xml.registration

