HTTP login service backend-requests API

Motivation

The http-util HttpLoginService interface provides a means for registering various login mechanism to be uset by teh gwt-sec library and other using OSGi /GWT.

There are implementations of HttpLoginService, which use LDAP (gwt-ladp-login-service) or JAAS (gwt-jaas-login-service) for authentication.

In order to allow for secure distributed authentication services with user-supplied backends, another HttpLoginService (gwt-http-login-service) will be implemented, which authenticates a user using a simple HTTPS request.

Authentication request

A request to an authentication URL is a HTTPS POST request

```
POST /my/authentication/service HTTP/1.1
Host: auth.my.domain
Content-Type: application/x-www-form-urlencoded

user=<user>&passwd=<passwd>
```

The user and password fields *must* not be tranferred as GET variables and the use of plain HTTP is strongly discouraged, an authentication service should always use HTTPS.

Authentication Response

An authentication must respond to an authentication request with an HTTP response with

```
Content-Type: text/plain; charset=utf-8
```

and on of the following status codes:

```
200 OK - successful authentication
403 Forbidden - if the user name or the password is wrong or no user and passwd field ist given.
406 Not Acceptable - The status, which will be returned after to many unsuccessful authentications.
```

The body of the response *must* no contain more than 1024 bytes and should contain a short, information text message encoded in UTF-8. The text message will be logged by the gwt-http-login-service bundle and will not be displayed to the user.

The server may enforce the use of HTTP basic authentication in order to keep offending servers away from dictionary attacks.