TYPO3.Flow - Feature #44563

Logged in users via HTTP Basic always get re-authenticated

2013-01-16 11:28 - Marco Falkenberg

Status:	New	**Start date:**	2013-01-16
Priority:	Should have	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Security	**Estimated time:**	0.00 hour
Target version:			
PHP Version:		**Complexity:**	
Has patch:	No		

Description

Logged in users via HTTP Basic will always be re-authenticated by the authentication provider manager, because the UsernamePasswordHttpBasic token always sets the authentication status either to "authentication needed" or "no credentials given".

There are two cons related to this fact:

1. After being logged in, every following request results in a new authentication which could (or better should) be very cheap depending on the used hashing strategy. Thus requests taking a long time and stressing the server.
2. Every requests results in changing to a new session.

A possible solution could be to narrow down the use of "authentication needed" and only re-authenticate under the following circumstances:

1. The username has changed.
2. The password has changed.

Detecting a change of the username is easy. Just store the logged in user in the token and compare it with the current.

Detecting a change of the password is the problem, because you should not store the last used password in the token (security). Also hashing the password is no good idea. Maybe you could ignore changes in password and rely on getting the same username password combination all over the time (or for a limited timespan).

Maybe some else has an idea how to solve this more deterministic?