TYPO3.Neos - Bug # 53989

Status:	Resolved	**Priority:**	Must have
Author:	Bastian Waidelich	**Category:**	
Created:	2013-11-26	**Assigned To:**	Bastian Waidelich
Updated:	2013-12-04	**Due date:**	
Subject:	user workspace must not be configurable		

Description

The user workspace is currently determined via

```
1$user = $this->securityContext->getPartyByType('TYPO3\Neos\Domain\Model\User');
2$userWorkspaceName = $user->getPreferences()->get('context.workspace');
```

This is error-prone and - as user preferences can be changed by the user - a security flaw.
I'd suggest following measures:

Get rid of the UserPreference entity

- This is just a serialized array, that could be in the user model - if we need it at all
- It is currently used for "context.workspace" and "contentEditing.wireframeMode" - both of which should not be in there

Centralize the users workspace logic

There is already **UserService::getCurrentWorkspace()** that could do what currently *UserFactory::create()* does:

```
1$workspaceName = 'user-' . preg_replace('/[^a-z0-9]/i', '', $username);
```

Even though this method is not yet called **once** in our code base.

Associated revisions

Revision 828e261c - 2013-12-03 20:22 - Bastian Waidelich

[BUGFIX] User workspace must not be configurable

This adjusts all parts of Neos that relied on a user preference
"context.workspace" to retrieve the current user workspace and moves
that logic into the already existing ``UserService``.

The reason for this is that logged in users are able to change their
preferences and we're currently lacking a validation for the configured
user workspace.

As of now a user only has access to one workspace (in addition to the
always accessible "live" workspace).
In the future a user might have access to more than one workspace and
we'll need to re-introduce some kind of workspace preference.

Change-Id: I53326e4b59654b6572397509220088cff7165d23

Fixes: #53989
Reviewed-on: https://review.typo3.org/25725
Reviewed-by: Aske Ertmann
Tested-by: Aske Ertmann
Reviewed-by: Christian Mueller
Tested-by: Christian Mueller

History

#1 - 2013-11-28 12:20 - Bastian Waidelich

- Status changed from New to Accepted

- Assigned To set to Bastian Waidelich

#2 - 2013-11-28 14:03 - Bastian Waidelich

BTW: This is a security flaw because user preferences can be changed via an ExtDirect call. And we shouldn't prohibit the user from changing it's preferences

#3 - 2013-11-28 14:05 - Gerrit Code Review

- Status changed from Accepted to Under Review

Patch set 1 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/25725

#4 - 2013-11-28 17:35 - Gerrit Code Review

Patch set 2 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/25725

#5 - 2013-11-28 19:00 - Gerrit Code Review

Patch set 3 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/25725

#6 - 2013-11-28 19:01 - Gerrit Code Review

Patch set 4 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/25725

#7 - 2013-12-03 19:19 - Gerrit Code Review

Patch set 5 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/25725

#8 - 2013-12-03 20:18 - Gerrit Code Review

Patch set 6 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/25725

#9 - 2013-12-03 20:22 - Gerrit Code Review

Patch set 7 for branch **master** of project **Packages/TYPO3.Neos** has been pushed to the review server.
It is available at https://review.typo3.org/25725

#10 - 2013-12-03 20:36 - Bastian Waidelich

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset commit:828e261c2c9d4dc1b31102284f1f911c06b5fcfe.

#11 - 2013-12-04 18:43 - Bastian Waidelich

- Target version set to 1.0 beta 2