TYPO3.Flow - Feature #45282

Work Package # 45088 (Resolved): Improved REST support

Support for "sessionless authentication"

2013-02-08 15:41 - Bastian Waidelich

Status:	Resolved	**Start date:**	2013-02-08
Priority:	Should have	**Due date:**	2013-04-13
Assignee:	Bastian Waidelich	**% Done:**	100%
Category:	Security	**Estimated time:**	108.00 hours
Target version:	2.1		
PHP Version:		**Complexity:**	
Has patch:	No		

Description

Currently Flow relies on a session to be active in at least three places:

1. \TYPO3\Flow\Security\Aspect\RequestDispatchingAspect::blockIllegalRequestsAndForwardToAuthenticationEntryPoints() calls \TYPO3\Flow\Security\Context::setInterceptedRequest() if an **entryPoint** is defined. Setting the intercepted request starts a session. This can be worked around by avoiding entryPoint or using requestPatterns to limit them only to certain parts of an application that allow sessions. #45100 might also be a solution for that
2. \TYPO3\Flow\Security\Authentication\AuthenticationProviderManager::authenticate() emits the authenticatedToken signal after successful authentication which is configured to call \TYPO3\Flow\Session\SessionInterface::renewId()
3. \TYPO3\Flow\Security\Authentication\AuthenticationProviderManager::isAuthenticated() returns FALSE if no session was started/can be resumed

Related issues:

Related to TYPO3.Flow - Feature #45100: RequestDispatchingAspect should check...	**Under Review 2013-02-03**

Associated revisions

Revision 7d79b800 - 2013-02-26 11:38 - Bastian Waidelich

[!!!][FEATURE] Support for "sessionless authentication"

This feature enables authentication without the need of a session to be started.
This is useful for stateless services (e.g. REST) where you don't want Flow to create
a session cookie.

This is a breaking change if you created a custom authentication provider or -token
and relied on the fact that AuthenticationProvider::authenticate() started a session.
With this change the session is started when AuthenticationToken::updateCredentials() is
called. This way the token can decide if it needs a session.
Just add a @Flow\Session(autoStart=true) to the updateCredentials() method if your custom
token relies on a session.

Change-Id: I5f86cb7a3a3fff3220d61d705f216e1b1d4f2369
Resolves: #45282
Releases: master, 2.0

Revision bd46c612 - 2013-03-05 13:23 - Bastian Waidelich

[BUGFIX] Fix security related functional tests

With the fix related to "sessionless authentication"
(I5f86cb7a3a3fff3220d61d705f216e1b1d4f2369) settings have been
adjusted in order to use the testing provider & token only for requests
matching a ControllerObjectName of "TYPO3\Flow\Tests\.*".

This change adjusts the tests accordingly.

Change-Id: I307cd295c43c346f18acc5c1fd2886166c10cbbb
Related: #45282
Resolves: #45953
Releases: master, 2.0

Revision 158f3519 - 2013-04-05 11:34 - Bastian Waidelich

[!!!][FEATURE] Support for "sessionless authentication"

This feature enables authentication without the need of a session to be started.
This is useful for stateless services (e.g. REST) where you don't want Flow to create
a session cookie.

This is a breaking change if you created a custom authentication provider or -token
and relied on the fact that AuthenticationProvider::authenticate() started a session.
With this change the session is started when AuthenticationToken::updateCredentials() is
called. This way the token can decide if it needs a session.
Just add a @Flow\Session(autoStart=true) to the updateCredentials() method if your custom
token relies on a session.

Change-Id: I5f86cb7a3a3fff3220d61d705f216e1b1d4f2369
Resolves: #45282
Releases: master, 2.0

Revision 6a94328f - 2013-04-05 11:34 - Bastian Waidelich

[BUGFIX] Fix security related functional tests

With the fix related to "sessionless authentication"
(I5f86cb7a3a3fff3220d61d705f216e1b1d4f2369) settings have been
adjusted in order to use the testing provider & token only for requests
matching a ControllerObjectName of "TYPO3\Flow\Tests\.*".

This change adjusts the tests accordingly.

Change-Id: I307cd295c43c346f18acc5c1fd2886166c10cbbb
Related: #45282
Resolves: #45953
Releases: master, 2.0

Revision 9feb5902 - 2013-04-05 17:06 - Robert Lemke

[FEATURE] Support for sessionless authentication

This feature enables authentication without the need of a session to
be started. This is useful for stateless services (e.g. REST) where
you don't want Flow to create a session cookie.

Authentication tokens which don't rely on a session simply implement
the SessionlessTokenInterface marker interface.

This patch reverts parts of the first implementation of sessionless
authentication introduced in https://review.typo3.org/#/c/18388
(commit I5f86cb7a3a3fff3220d61d705f216e1b1d4f2369).
The original implementation was a breaking change with a few
unresolved side effects.

The implementation contained in this change set is backwards
compatible with already existing authentication tokens which
relied on sessions.

This patch also contains a small speed optimization for the CSRF
Protection pattern which assumes that no account has been
authenticated yet if the Authentication Manager is still a Dependency
Proxy.

Change-Id: Iccd2b8fde6a5f37d3d434c959705a85cdcda4b11
Resolves: #45282
Resolves: #46428
Releases: master, 2.0

Revision ff5de86a - 2013-04-05 20:05 - Robert Lemke

[FEATURE] Support for sessionless authentication

This feature enables authentication without the need of a session to
be started. This is useful for stateless services (e.g. REST) where
you don't want Flow to create a session cookie.

Authentication tokens which don't rely on a session simply implement
the SessionlessTokenInterface marker interface.

This patch reverts parts of the first implementation of sessionless
authentication introduced in https://review.typo3.org/#/c/18388
(commit I5f86cb7a3a3fff3220d61d705f216e1b1d4f2369).
The original implementation was a breaking change with a few
unresolved side effects.

The implementation contained in this change set is backwards
compatible with already existing authentication tokens which
relied on sessions.

This patch also contains a small speed optimization for the CSRF
Protection pattern which assumes that no account has been
authenticated yet if the Authentication Manager is still a Dependency
Proxy.

Change-Id: Iccd2b8fde6a5f37d3d434c959705a85cdcda4b11
Resolves: #45282
Resolves: #46428
Releases: master, 2.0

History

#1 - 2013-02-19 22:20 - Gerrit Code Review

- Status changed from New to Under Review

Patch set 1 for branch **master** has been pushed to the review server.
It is available at https://review.typo3.org/18388

#2 - 2013-02-22 10:37 - Bastian Waidelich

- Parent task set to #45088

#3 - 2013-02-26 11:38 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at https://review.typo3.org/18388

#4 - 2013-02-26 17:36 - Bastian Waidelich

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset 7d79b800d4237a359d3876a69538078dc2298d18.

#5 - 2013-03-20 17:24 - Gerrit Code Review

- Status changed from Resolved to Under Review

Patch set 1 for branch **2.0** has been pushed to the review server.
It is available at https://review.typo3.org/19106

#6 - 2013-03-27 08:53 - Gerrit Code Review

Patch set 1 for branch **master** has been pushed to the review server.
It is available at https://review.typo3.org/19340

#7 - 2013-03-27 10:23 - Gerrit Code Review

Patch set 2 for branch **master** has been pushed to the review server.
It is available at https://review.typo3.org/19340

#8 - 2013-03-28 16:21 - Aske Ertmann

- Parent task deleted (#45088)

#9 - 2013-03-28 16:22 - Aske Ertmann

- Parent task set to #45088

#10 - 2013-03-28 16:29 - Aske Ertmann

- Estimated time set to 108.00 h

#11 - 2013-04-02 13:17 - Bastian Waidelich

- Due date set to 2013-04-13

#12 - 2013-04-05 11:36 - Gerrit Code Review

Patch set 2 for branch **2.0** has been pushed to the review server.
It is available at https://review.typo3.org/19106

#13 - 2013-04-05 11:38 - Bastian Waidelich

- Status changed from Under Review to Resolved

Applied in changeset 158f3519fd043533c3deef8dbc300527a0020490.

#14 - 2013-04-05 17:10 - Gerrit Code Review

- Status changed from Resolved to Under Review

Patch set 3 for branch **master** has been pushed to the review server.
It is available at https://review.typo3.org/19340

#15 - 2013-04-05 17:36 - Anonymous

- Status changed from Under Review to Resolved

Applied in changeset 9feb5902e1c4ed1b32278b28b6edc0a41a6bb7b9.

#16 - 2013-04-05 20:14 - Gerrit Code Review

- Status changed from Resolved to Under Review

Patch set 1 for branch **2.0** has been pushed to the review server.
It is available at https://review.typo3.org/19615

#17 - 2013-04-05 20:37 - Anonymous

- Status changed from Under Review to Resolved

Applied in changeset ff5de86a050865abee0fb5c860261c66710b74f5.