TYPO3.Comments - Task # 34666

Status:	Accepted	**Priority:**	Must have
Author:	Adrian Föder	**Category:**	
Created:	2012-03-08	**Assigned To:**	
Updated:	2012-03-09	**Due date:**	
Subject:	Reconsider the handling of persons/parties		

Description

With the current implementation, a new comment's author's given first name and email address is gathered as data for retrieving a probably already existing Person instance.

If such a Person entity is used in various contexts at the platform, this might result in a security issue, because you could slip into that user's representation just with spoofing the first name and email address.

So, how could this be prevented?

One use case may be that the author of a comment **must always** be the authenticated user. But if that's not needed, what then? Make that behavior configurable?

Please post any ideas you have.

History

#1 - 2012-03-08 12:23 - Bastian Waidelich

- Status changed from New to Accepted

Maybe a setting @allowCreationOfNewUsers" (or similar) would work out..
For flow3.org we need comments without authentication

#2 - 2012-03-09 14:58 - Adrian Föder

with further thinking about it; maybe it makes sense to change a comment to have first name, email and person handled parallelly, maybe with

```
\Comment:
  /* @var \TYPO3\Comments\Domain\Model\AbstractAuthor */
  $author;

\AuthenticatedAuthor extends \AbstractAuthor
  /* \TYPO3\Party\Domain\Model\AbstractParty
  $party

\AdHocAuthor extends \AbstractAuthor
  /* @var string */
  $firstName
  /* @var string */
  $emailAddress
```

because I really see a danger to take over a \Person which may be bound to an account! or other profile data, just by an unverified email address and

first name.

So, because of the fact that TYPO3.Party is so much bound to authentication stuff, I'd really recommend to store the given data (email addr. and firstname) as they are: as strings next to each other.
If the package can't guarantee that a person isn't a person, it should reflect that fact and only display name and email address as-is.