Basic Terms

by Andreas Hartmann

1. Role

*Role*s are the connection between access control and CMS functionality. On the access control side, you assign *Role*s to users, IP address ranges and groups at certain URL spaces. On the CMS side, you define which *Role*s are needed to execute certain usecases and workflow transitions. If the client has a certain *Role*, this means he is allowed to do something.

Each *Role* has a unique name. Role names can be arbitrary strings. Examples are

- author
- reviewer
- admin

Another common approach and useful is to use verbs as role names:

- edit
- review
- administrate

2. Identifiable

An *Identifiable* is a characteristic of the client that can be identified. Every *Identifiable* is *Accreditable*. Lenya currently supports the following *Identifiable*s:

- users
- machines
- the world (this idenitifiable is assigned to every client that tries to access the system)

3. Identity

An *Identity* is the collection of all *Identifiable*s that have access to the system in the current session. The *Identity* always contains the world and the machine that produced the request. If you logged in, the user is also contained in the *Identity*.

For instance, if you log in from the machine 192.168.0.16 as the user john, the *Identity* of the client contains

- the machine 192.168.0.16,
- the user john, and
- the world.

4. Accreditable

An *Accreditable* can be accredited with *Role*s in *Policies*. Lenya currently supports the following *Accreditable*s:

- users
- machines (accredition not implemented, use IP ranges instead)
- IP address ranges
- the world
- groups

5. Credential

A *Credential* assigns a set of *Role*s to an *Accreditable*, e.g.:

- `news_editors: editor, reviewer`
  means "The group `news_editors` has the *Role*s `editor` and `reviewer`."

6. Policy

A *Policy* defines a set of *Credential*s for a certain URL. It has the responsibility to return all *Role*s of an *Accreditable* at a certain URL.

If for instance the *Policy* for the URL /tv/news contains the *Credential*s

- `news_editors: editor, reviewer`
- `john: admin`
- `192.168.0.72: visitor`

and user `john` belongs to the group `news_editors` and has logged in from the machine `192.168.0.72`, the *Policy* returns the *Role*s `editor, reviewer, admin, visitor` for the *Accreditable* `john`.

A *Policy* may not contain invalid *Accreditable*s. E.g., if a user is deleted and another user with the same ID is created, he may not get the same privileges as the former one.