Basic Terms

by Andreas Hartmann

1. Role

Roles are the connection between access control and CMS functionality. On the access control side, you assign roles to users, IP address ranges and groups at certain URL spaces. On the CMS side, you define which roles are needed to execute certain usecases and workflow transitions.

Examples of roles are

- author
- editor
- admin

2. Identifiable

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

- 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 Identifiables 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, your identity contains this machine, this user and the world.

4. Accreditable

An Accreditable can be accredited with roles at URLs. Lenya currently supports the

lowing accreditables:

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

5. Credential

A Credential assigns a set of Roles to an Accreditable, e.g.:

- `news_editors: editor, reviewer` means "The group `news_editors` has the roles `editor` and `reviewer`."

6. Policy

A Policy defines a set of Credentials for a certain URL. It has the responsibility to return all Roles of an Accreditable at a certain URL.

If for instance the policy for the URL /tv/news contains the credentials

- `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 set `editor, reviewer, admin, visitor` for the accreditable `john`.

A policy may not contain invalid accreditables. 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.