Identity & Access Control Management Infrastructure Blueprint - Design Principles for True Informational Self-Determination

by Daniel Pluta, Wolfgang Hommel, and Peter Weinert

In our paper, we specified the design criteria and presented the reference implementation of an identity & access control management infrastructure that does not only offer self-service functionality to all of its users, but achieves true informational self-determination. Privileged proxy-users, which are . as we have shown . by their design conflicting with informational self-determination, are completely forgone. Each user stays in full control of which personal data is shared with which other users or services in the granularity of LDAP attributes. Additionally, each user is free to express her individual will regarding all resources she is responsible for, while maintaining an overall state of individual responsibility. As a direct result of our self-determination-driven design principles, our approach aligns smoothly with the identity management requirements of modern businesses and their respective IT service providers.

In this talk, we first motivate our design by summarizing the deficiencies inherent to the identity management systems that are in use today, and explain why they do not achieve informational self-determination. Based on a clarification why informational self-determination is our overall goal, we present the technical requirements and our design principles. Afterwards, we discuss the technical aspects of our reference implementation: Our infrastructure is based on OpenLDAP as its backend; it makes heavy use of OpenLDAP.s impressive ACL engine to ensure that no additional access control is required outside this back-end. Furthermore, we present our front-end prototype. However, as there are no privileged proxy-users, any user could also implement an alternative (graphical) user interface and still harvest the system.s full functionality. After a summarizing overview of the resulting infrastructure.s complete architecture, we discuss our results and the open issues that we will address in future work.