PROFIDATA GROUP

XENTIS Fact Sheet

Centralised User Administration with XENTIS Lightweight Directory Access Protocol

XENTIS supports the Single-Sign-on procedures: after logging in to the corporate network for the first time, no additional log-in to XENTIS is necessary. The Lightweight Directory Access Protocol LDAP supplements the variant Silent-Sign-on in conjunction with a centralised user administration system.

Background

Themes such as user administration, authorisation (issue of user privileges), user authentication (proof that a user is exactly who they claim to be in the IT system) and IT authentication (automatic check of the user's security information by the IT system) are directly connected with IT security and therefore play a crucial role in a company's IT audit procedures. The respective IT security procedures need to be defined in detail and if possible used for all the applications running on the IT infrastructure. From an audit perspective, for example, it is vital to ensure that once a member of staff leaves the company not only are all transactions blocked on their account, but all the respective user authorisations are deleted as well.

The following Single-Sign-on variants are available in XENTIS:

1. With the **Silent-Sign-on** variant, the user is initially authenticated by means of their workstation. On start-up, the XENTIS client receives the user details required to establish the connection with the XENTIS server. Once the user has been successfully authenticated by the XENTIS server,

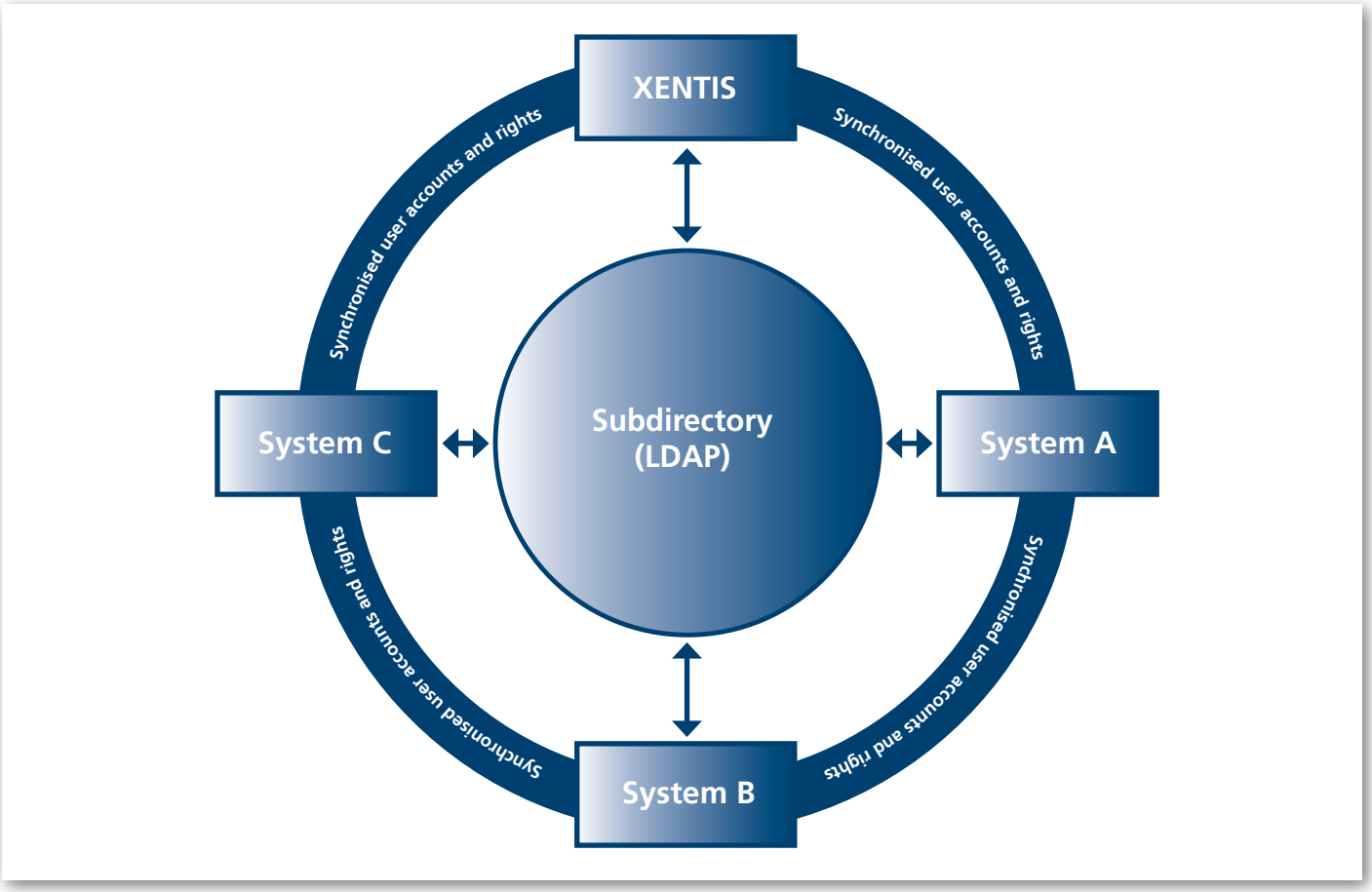

Fig. 1: IT authentication of the user and synchronisation of the user accounts and user rights

they are able to log in to XENTIS without entering a password. The benefits of this variant include the fact that it is inexpensive to set up and simple to run. The attention given to security aspects is fairly limited, however. Therefore, the Silent-Sign-on variant can be supplemented by an exchange of X.509 certificates. A dedicated server is integrated in the log-in procedure for IT authentication purposes. XENTIS passes the user's log-in information to this server, which verifies that they are correct and then confirms the user's authenticity. Although this procedure offers a more advanced means of IT authentication, it does require a dedicated infrastructure. This variant offers a high level of security and tends to be suitable for audit purposes. However, an employee's user account is not automatically deleted when they leave the company.

2. With the **LDAP variant**, both IT authentication and authorisation can be transferred to an LDAP directory, such as the commonly used Microsoft Active Directory. The administration of users and their privileges therefore occurs in the centralised authorisation environment of the individual company, in other words the privileges are assigned to users in the LDAP server by the person(s) responsible for granting authorisation. The definition of the respective roles and rights is actually handled in XENTIS, however. When the user logs in to XENTIS, it is not therefore XENTIS which performs the IT authentication: the details are forwarded in the form of a request to the centralised user administration facility. This request hardly takes any longer than IT authentication performed directly by XENTIS. At the same time as IT authentication, the user roles and rights defined in XENTIS are synchronised with the roles specified in centralised user administration (**Fig. 1**) and any changes made to privileges immediately updated in the latter. In a scenario where an employee is leaving the company, this arrangement ensures that the relevant user account is automatically deleted. This variant provides the highest standard of security and is fully compliant with audit requirements.

Conclusion

The integration of LDAP in XENTIS permits the use of centralised user administration based on the automatic synchronisation of the users managed in XENTIS. This ensures consistent administration of user privileges and user accounts. If clients prefer an alternative Single-Sign-on procedure, XENTIS offers the additional variant Silent-Sign-on.

For further information, please contact

Peter Klein
Member of the Management Board
phone +41 44 736 47 90
peter.klein@profidatagroup.com