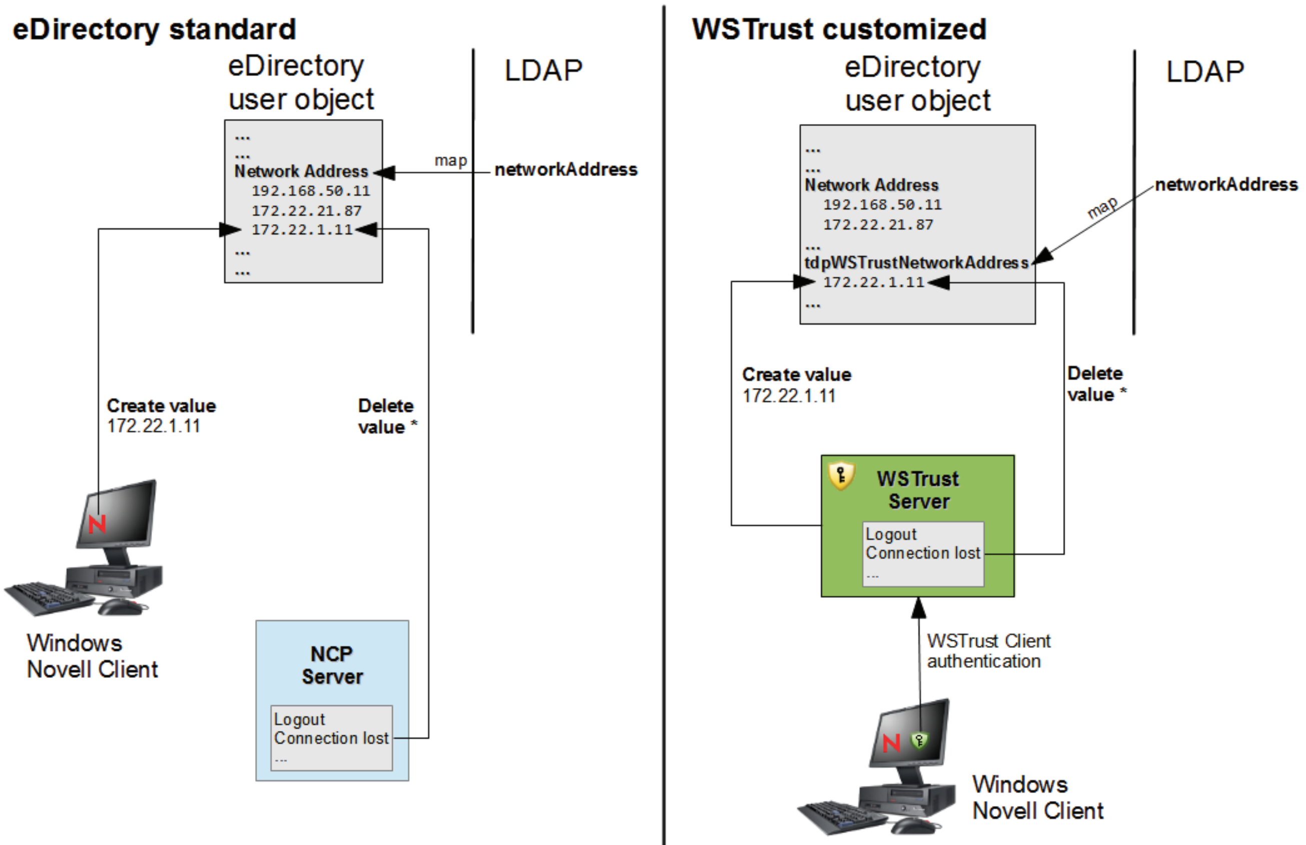
case study

KeyShield SSO networkAddress solution supports IronPort SSO at Ministry of Interior, CZ

Ministry of Interior Czech Republic (hereinafter referred to as MI) uses the IronPort web security gateway for monitoring and controlling access to the Internet. It was working well; but Mr. Vladimir Vosicky, head of the ICT dept. of MI decided to implement SSO authentication for IronPort users, for two main reasons. The first was work efficiency – when users have to log in repeatedly, they waste time and concentration. Secondly, there were technical problems with redirection to the authentication dialog of IronPort in the case of a timeout. If the user had been working in a secure system and there was a timeout (for example, due to the preparation of documents), users were not able to continue the original session after reauthentication to the proxy server..

The MI environment is based on Novell infrastructure technologies: users authenticate to eDirectory. Like many similar solutions, IronPort offers SSO authentication for eDirectory based on the multi-value networkAddress attribute of user objects. Unfortunately, this attribute was never designed or upgraded to be suitable for SSO functionality. The value of the attribute is created by the Novell Client for Windows during the authentication process. The value is then removed from eDirectory by the NCP server, but the server‘s ability to maintain all possible situations is limited. Therefore this networkAddress attribute is not sufficiently reliable for SSO authentication. This was confirmed not only through an operational test carried out at MI, but also by comparing experiences with users of other solutions which rely on a networkAddress attribute.

Because the IronPort system has no other suitable SSO interface for an eDirectory enviroment, Mr Vosicky actively sought a solution which would provide reliable and secure networkAddress attribute handling where IronPort was already installed. We were



* Oftenly fails due to non-standard connection abort

* 100% Reliable, no Ghost IP Addresses

approached for a solution, along with other potential suppliers. Because KeyShield SSO is fully integrated with eDirectory, we came up with the solution in the diagram.

We created our own eDirectory auxiliary Class with a multi-value tdpWSTrustNetworkAddress attribute. This attribute is managed directly by the KeyShield SSO server, so it is as safe and reliable as authentication through the KeyShield SSO server itself. Admin can configure the replica server which KeyShield SSO uses to handle the attribute - ideally of course the one that reads IronPort or a similar system. Alternatively, admin can just change the configuration of replication of this attribute from slow to fast. In addition, we have changed the LDAP attribute mapping interface to an LDAP attribute that is not mapped to the original, but to the new networkAddress attribute - tdpWSTrustNetworkAddress. Thus, what we have achieved through the LDAP interface is to read the KeyShield SSO server-handled attribute without affecting the functionality of systems that use the attribute - in this case, IronPort. The difference between the standard and modified attribute networkAddress solution is shown in the diagram.

The KeyShield SSO server was then installed in an operational environment at MI, and integration with IronPort was subjected to intensive testing for two months. All tests passed without the slightest error, and subsequently MI launched IronPort SSO authentication against KeyShield SSO / networkAddress. Now the KeyShield SSO system is also used for authentication to the Retain archive system.