

Kerberos PKINIT implementation on Linux

The Client

The customer is a business unit of a NYSE listed company, which is a leading oilfield services company supplying technology, project management and information solutions that optimize performance for their customers working in the international oil and gas industry.

The Challenge

The KERB system responsible for communicating between the Smart Card and the KDC to procure the Ticket Granting Ticket [TGT] used to access different services or applications. The objective was to implement this system on the Linux platform using the Public Key Cryptography for Initial Authentication in Kerberos [PKINIT]. It should also be implemented as a Pluggable Authentication Module [PAM] on Linux.

The Solution

- LINUX clients will be able to access the Windows services when they logon to the LINUX workstation
- Users can authenticate their identity on Linux using their Windows 2000 Domain credentials.
- Users can use their Windows 2000 Domain credentials (In the form of a TGT) to access Kerberized UNIX Services.
- Strong authentication technology - an attacker listening to the network gains no information that would enable it to impersonate the user
- Provides additional security services of integrity, confidentiality and authorization

The Benefits

- Provide solution for PKINIT using Kerberos on Linux platform
- From the LINUX workstation, clients will be able to securely access their Windows services and to securely access Kerberized UNIX Services

The Technology

Kerberos on Linux platform