Chapter XI

Portlet Authentication and SSO

In this section, we will introduce a few important details relevant to the authentication process and Single Sign On (SSO) implementation. The SSO is a popular feature that was established in the portal standard JSP 168 as a mandatory feature. This functionality enables the user to authenticate only once to all Web services and back-end applications to which he or she requires access. The authentication code is propagated to all services for which the user has access permissions. This means that users can log on only once and be known to the various parts of the portal server with the same user credentials.

Authentication Process

Authentication can be loosely defined as the process of establishing a user’s identity and verifying credentials. In a portal environment, authentication may be achieved by providing a unique user name and password pair. The user is assigned a certificate that is validated by using a third-party authentication server, or a smart card or biometric device (Figure 105). The final solution may involve all three methods, and it will require a repository integrated with the system and holding these identities. For example, the WebSphere portal server...
uses the authentication services provided by the WebSphere Application Server and CORBA credentials together with an encrypted Lightweight Third Party Authentication (LTPA) cookie to authenticate users. Alternatively, it is possible to authenticate via an LDAP directory, which may hold some application-oriented attributes in addition to authentication information, that is, a hierarchical reporting structure.

The actual situation with portlets is more complicated. The portal provides an integrated view of multiple back-end applications, and, sometimes, access to Web services. Web services typically access additional data resources on behalf of the portal user, which may in turn retrieve further data from other data sources on behalf of this user. In this case, the user’s credentials are presented to the Web services by the portlet of the portal page into which the user is logged on.

The area of security is widely covered in books. The Secure Socket Layer (SSL) and Transport Layer Security (TLS) were introduced by Netscape in 1994 as a response to the growing concern over security on the Internet. XML Encryption and XML Signature are W3C standards, which can be used to encrypt elements of an XML document and prove message integrity. Any part of an XML document can be digitally signed, and it becomes self-validating when the document recipient has the signer’s public key. An OASIS standard, the Security Assertion Markup Language (SAML) is used to pass authentica-