Diff notes: SAML 2.0 Kerberos Attribute Profile (OASIS SSTC)

Authors: Josh Howlett (Individual) and Thomas Hardjono (MIT)

Date of this note: December 15, 2010

The SAML 2.0 Kerberos Attribute Profile (CD-01) was modified substantially due to the need to satisfy a request from developers at CMU regarding the use of an unencrypted KRB-CRED structure.

RFC4120 that specifies the Kerberos V5 protocol assumes that the KRB-CRED structure is an encrypted structure, which contains a number of sensitive data fields. However, in the CMU use-case there is the situation in which a trusted entity in the infrastructure is required to hold an unencrypted (plaintext) KRB-CRED structure (for future usage on behalf of the client principal). This usage of an unencrypted KRB-CRED has been discussed in the past in the IETF Kerberos WG, but no formal specification had been created. As such, the CMU authors submitted a proposed specification for this KRB-CRED usage to the IETF (see reference [NonEncKrb]).

The relevant new text within the SAML 2.0 Kerberos Attribute Profile are the following (in Section 2.7):

The KRB-CRED message contains sensitive information related to Kerberos credentials being transferred, such as their secret session keys, client and server principal names, and validity period. Posession of this information, along with the ticket itself, would allow an attacker to impersonate the client named in the ticket. As a result, this information must be carefully safeguarded.

The definition of the KRB-CRED message in section 5.8 of [RFC4120] provides for protection of the confidentiality and integrity of the sensitive portions of the KRB-CRED message when it is passed in the context of a previous Kerberos authentication, by encrypting those portions in a key derived from the shared Kerberos session key. When the issuer and recipient of this attribute share an appropriate Kerberos authentication context, it SHOULD be used to protect the KRB-CRED message as described in [RFC4120].

However, the issuer and recipient of a SAML attribute often do not share an Kerberos authentication context. To facilitate use of this attribute in such cases, the non-encrypted form of the KRB-CRED message [NonEncKrb] may be used. When the non-encrypted form is used, the confidentiality and integrity of the message MUST be protected by alternate means such as Transport Layer Security (TLS) or the <EncryptedAttribute> element.

To facilitate interoperability, implementations of this profile MUST support sending and receiving the non-encrypted form of the KRB-CRED message, and MUST support protection of this attribute by use of the <EncryptedAttribute> element.