kitten
Charter Work Items

Shawn Emery (shawn.emery@oracle.com)

Existing Work Items

- SASL Mechanism for OAuth (draft-ietf-kitten-sasl-oauth)
- SASL Mechansim for SAML-EC (draft-ietf-kitten-sasl-saml-ec)
- GSS-API IANA Registry (draft-ietf-kitten-gssapi-extensions-iana)
- KDC Model (draft-ietf-krb-wg-kdc-model)
- PKINIT Hash Agility (draft-ietf-krb-wg-pkinit-alg-agility)
- Kerberos Referrals (draft-ietf-krb-wg-kerberos-referrals)
- Kerberos Options for DHCPv6 (draft-sakane-dhc-dhcpv6-kdc-option)
- Camellia Encryption for Kerberos 5 (draft-ietf-krb-wg-camellia-cts)
- Kerberos IANA Registry (draft-ietf-kitten-kerberos-iana-registries)

GSS-API Related

- Provide new interfaces for credential management, which include the following:
  initializing credentials
  iterating credentials
  exporting/importing credentials

- Negotiable replay cache avoidance

- Define interfaces for better error message reporting.

- Specify an option for exporting partially-established security contexts and possibly a utility function for exporting security contexts in an encrypted form, as well as a corresponding utility function to decrypt and import such security context tokens.

Kerberos Related

- Prepare, review, and advance standards-track specifications defining use of updates and extensions to RFC4121 in Kerberos, on an ongoing basis.

- Prepare and advance one or more standards-track specifications which update the Kerberos version 5 protocol to support non-ASCII principal and realm names, salt strings, and passwords, and localized error reporting. Maximizing backward compatibility is strongly desired.

- Prepare and advance one or more standards-track specifications which update the Kerberos version 5 protocol in a backward-compatible way to support extending the unencrypted portion of a Kerberos ticket.

Kerberos Related (2 of 3)

- Prepare, review, and advance standards-track and informational specifications defining new authorization data types for carrying supplemental information about the client to which a Kerberos ticket has been issued and/or restrictions on what the ticket can be used for. To enhance this ongoing authorization data work, a container format supporting the use cases of draft-sorce-krbwg-general-pac-01 may be standardized.

- Prepare a standards-track protocol to solve the use cases addressed by draft-hotz-kx509-01 including new support for digital signatures.

- Today Kerberos requires a replay cache to be used in AP exchanges in almost all cases. Replay caches are quite complex to implement correctly, particularly in clustered systems. High-performance replay caches are even more difficult to implement. The WG will pursue extensions to minimize the need for replay caching, optimize replay caching, and/or elide the need for replay caching.

Kerberos Related (3 of 3)

- Prepare, review, and advance standards-track and informational specifications defining use of new cryptographic algorithms in the Kerberos protocol, on an ongoing basis.

- Prepare, review, and advance standards-track and informational specifications defining use of new cryptographic algorithms in Kerberos using the RFC3961 framework. Cryptographic algorithms intended for standards track status must be of good quality, have broad international support, and fill a definite need.

- Prepare, review, and advance standards-track and informational specifications of new pre-authentication frameworks for the Kerberos protocol, on an ongoing basis.