IETF67 Kitten Working Group

Jeffrey Altman - Chair
jaltman@secure-endpoints.com
Preliminaries

• Introduction
• Blue Sheets
• Scribe(s)
• Agenda Bashing
Meeting Resources

• Jabber
  – Room: kitten   Server: jabber.ietf.org

• Presentation Materials

• Audio Streaming
  – http://videolab.uoregon.edu/events/ietf/ietf672.m3u
Agenda

1. Document Status
2. Charter and Milestone Revision Status
3. Internationalization
4. Open Microphone for Technical Discussions
5. Presentations on Related Technologies
   1. PKU2U and WSKERB – Larry Zhu
IETF Last Call
GSS-API Domain Name docs

• Outstanding AD comments
• No IANA section yet a new OID allocation request is made
  – There is no IANA registry for the 1.3.6.1.5.6 sub-tree. Remove allocation request. Allocate by standards action.
• Recommend _foo._tcp.example.tld instead of just example.tld for DNS SRV lookups?
  – DNS SRV records require the _service._proto.fqdn notation
• Request replacement text for:
  – the realm of the resulting principal name is that which corresponds to the domain name, treated as a hostname.

• Proposed replacement:
  – the realm of the resulting principal name SHALL be that which would be used for a hostname whose name is the same as the domain name component of the domain-based service name.
WGLC: An Update to the Java GSS-API Specification

• Cannot pass last call without sufficient review.
• The only review has come from the editor, one of her reports, and the Chair
• The Chair has begun circulating the document outside the IETF for review
• Review from GSS-API experts must be received before this document can progress
WGLC Stackable Mechs / Extended Mech Inquiry APIs

• Martin Rex does not like reviving GSS_Release_OID() because of memory management issues
  • But GSS buffer management already has these issues and they’re not going away

• Martin also points out problems with minor status code namespaces
  • SPNEGO already has this problem and we know about it
  • We should treat minor status codes as dynamically allocatable opaque objects (note: pointers not needed)
WGLC Stackable Mechs / Extended Mech Inquiry APIs

• David Leonard had some minor comments and then asked about G11N
  – Will update I-D to follow the consensus from the G11N thread
  – See slide on G11N...
WGLC Stackable Mechs / Extended Mech Inquiry APIs

• Derek Atkins asks
  – Whether composition order matters
    • it does and is implied by composition rules
  – Why no formal composition rule language
    • Stackable mechs are expected to evaluate their own composition rules with respect to proposed compositions
    • Text explaining that frameworks would call on stackable mechanisms to do this (using their extended inquiry APIs) would probably be very helpful

• Derek points out that the extended mech. inquiry APIs I-D lacks a security considerations section
Charter and Milestone
Revision Status

• Sent to IESG; Currently being reviewed
• Charter Changes
  – Removes work item for definition of channels for IPSec, TLS, etc. This work is being completed as individual drafts
  – Adds permission to address Internationalization issues within GSS-API
GSS-API G11N

• After a long & painful debate we concluded that
  – GSS_Display_name/status() must be left as is.
    • Defined as ISO Latin-1.
    • Implementors that disregard the rules should document what they do

Date: Tue, 23 Jan 96 11:05:35 EST
From: "John Wray, Digital DPE"
Subject: Re: question on draft-ietf-cat-gssv2-cbind-01 [...] 
• ii) possible future I18N support. Today's GSSAPI assumes that character
•: strings are simple ISO-latin1 strings. At some time in the future, we may
•: want to support alternate character sets, using either multi-byte or wide
•: characters. Names are the most likely target for I18N, and APIs that support
•: extended character sets should behave as similar as possible to the regular
•: ISO-latin1 versions. NUL-termination doesn't work with wide characters.
GSS-API G11N

– New *_unicode() versions of those functions are needed
  • They return Unicode strings; encoding depends on language bindings (UTF-8 for C, UTF-16 for Java, ...)
  • Message L10N to the language of the caller’s locale

– New optional *_locale() versions of those
  • Use codeset/encoding of the caller’s locale
GSS-API G11N

- New functions that output human-readable strings should output Unicode strings
  - Messages should be localized to the language of the caller’s locale
- Optional *locale() versions of such new functions use codeset/encoding of caller’s locale
Upcoming WGLCs

• GSS-APIv2 Extension for Storing Delegated Credentials
Open Mic
Related Technology Presentations

1. PKU2U and WSKERB – Larry Zhu
Finished

Where are the Blue Sheets?