

# GSS-API Next Generation (kitten-wg) Chicago, IL – IETF 69th

Alexey Melnikov ([alexey.melnikov@isode.com](mailto:alexey.melnikov@isode.com))  
Shawn Emery ([shawn.emery@sun.com](mailto:shawn.emery@sun.com))

# Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- \* the IETF plenary session,
- \* any IETF working group or portion thereof,
- \* the IESG, or any member thereof on behalf of the IESG,
- \* the IAB or any member thereof on behalf of the IAB,
- \* any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,
- \* the RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 3978 (updated by RFC 4748) and RFC 3979(updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 3978 (and RFC 4748) for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

# Overview

- Introduction
- New Co-Chairs Announcement
- Blue Sheets
- Scribe, Jabber
- Remote Participation
- Agenda Bashing
- Active WG Items (30 – 60 minutes)
- Future Work Items (30 – 40 minutes)
- Review and Milestones (10 minutes)

# Active WG Items

- GSS-Domain draft-ietf-kitten-gssapi-domain-based-names
  - IESG in Sep
- KRB-Domain draft-ietf-kitten-krb5-gssapi-domain-based-names
  - IESG in Sep
- GSS-Channel draft-ietf-kitten-gssapi-channel-bindings
  - WGLC in Oct
- Mech-query draft-ietf-kitten-extended-mech-inquiry
  - IESG in Oct
- Pseudo-mech draft-ietf-kitten-stackable-pseudo-mechs
  - IESG in Nov
- Naming-ext draft-ietf-kitten-gssapi-naming-exts
  - WGLC in Nov
- Store-cred draft-ietf-kitten-gssapi-store-cred
  - WGLC in Dec
- Java-bind draft-ietf-kitten-rfc2853bis
  - WGLC in Jan

# Active WG Items (Issues)

- draft-ietf-kitten-gssapi-domain-based-names
  - Issues in IESG
- draft-ietf-kitten-krb5-gssapi-domain-based-names
  - Issues in IESG
- draft-ietf-kitten-gssapi-store-cred
  - Move forward with draft (pretty much ready)
- draft-ietf-kitten-rfc2853bis
  - Updates submitted based on review comments

# draft-ietf-kitten-gssapi-domain-based-names-03

- DISCUSSEs:
  - Domain based names syntax in ABNF?
  - Clarify: GSS service names, not port names
  - Fix examples (RFC2606)
  - I18N
    - What's a domainname slot, what's not?
      - If domain and/or hostname are, then IDNA
      - Else UTF-8
        - Deal w/ GSS\_Import/Display\_name() I18N

# IDNA or UTF8?

- Domain name and/or host name slots could use IDNA (ACE)
  - Harder for apps, perhaps?
  - Harder for mechs?
- Service name is ASCII only

# draft-ietf-kitten-krb5-gssapi-domain-based-names-03

- Affected by decisions on draft-ietf-kitten-gssapi-domain-based-names
  - NOTE: can't do I18N here w/o Kerberos I18N

# draft-ietf-kitten-rfc2853bis-05

- Editor will add appendix A, which lists the changes since RFC 2853

# draft-ietf-kitten-gssapi-channel- bindings-02

- Needs to be aligned with updates to draft-williams-on-channel-bindings
- Needs to be aligned with updates to TLS channel bindings I-Ds

# draft-ietf-kitten-stackable-pseudo-mechs-02

- Lots of work needed
- Consumers?
  - Pseudo-mechs make up for app protocol shortcomings. But are app protocols easier to extend/fix?

# draft-ietf-kitten-extended-mech- inquiry-02

- Several TBDs (base OID, intro and sec cons text)
- But closer than stackable pseudo-mechs I-D

# draft-ietf-kitten-gssapi-naming-exts-02

- TBD: AD-AND-OR authorization data must be mapped to a single critical attribute
- TBD: Base OID for auth-data type
- TBD: How to handle negative auth-data types
- Need text on x-realm transit paths
- PKIX stuff: time to move out into separate doc, or leave that to later?

# draft-ietf-kitten-gssapi-extensions-iana-01

- Lots of non-standard extensions (MIT has some, Sun has some, ...)
  - We need a registry
- Needs review of registration form, procedure
- Needs review of initial prefix registrations
- Needs initial contents (or can the registry be populated w/o initial contents being in an RFC?)

# Future Work Items

- Need editor and reviewers for the C#-bindings draft
- Need document/editor for C-bindings draft
- Alias list discussions
  - Mechanisms? (re-charter?)
  - draft-josefsson-password-auth-00
  - GSS-API application context handles
  - PKU2U
  - Sundry extensions

# draft-josefsson-password-auth-00

- Interest in future work with password based GSS-API mechanism?
- If so should we recharter?

# Review and Milestones

Do the goals and milestones look reasonable?