

# Common Authentication Technology Next Generation (kitten) Orlando, FL – IETF 86

Sam Hartman (hartmans-ietf@mit.edu)  
Shawn Emery (shawn.emery@oracle.com)  
Josh Howlett (josh.howlett@ja.net)

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

All IETF Contributions are subject to the rules of RFC 5378 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 5378 and RFC 3979 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

- Preliminaries (5 min)
  - Introduction
  - Blue Sheets
  - Scribe, Jabber
  - Remote Participation
  - Agenda Comments
- Kitten and Krb-wg Merger
- Active WG Items (15 min)
- SASL-OAuth Updates (15 min)
- Kerberos Registry to IANA (15 min)
- New Drafts Proposed (30 min)
- Open mic (5 min)
- GSS-Profiles (15 min; time permitting)

# Kitten and Krb-wg Merger

- New charter has been approved
- The Krb-wg list has been migrated to kitten
- Are there other tools related issues to be aware of with the move?

# Active WG Items

- IANA-reg (draft-ietf-kitten-gssapi-extensions-iana)
- SASL-SAML-EC (draft-ietf-kitten-sasl-saml-ec)
- 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)

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

- Leif had reviewed and comments on 07
  - Do changes warrant another WGLC?
  - Any other reviewers before we send to IESG?

# draft-ietf-kitten-sasl-saml-ec

- 06 had been submitted
  - Simplified session key schema
  - Random-to-key moved to end-points
  - Advertisement of session key and enc type by acceptor

# draft-ietf-krb-wg-kdc-model

- RFC Ed Queue

## draft-ietf-krb-wg-pkinit-alg-agility

- A few updates needed
  - RFC 3766 and RFC 6194 should be informative
  - Error code 82 conflict should be reassigned
    - Deployed code but impact unlikely

## draft-ietf-krb-wg-kerberos-referrals

- Now RFC 6806!
- Thanks to all

## draft-sakane-dhc-dhcpv6-kdc-option

- Now RFC 6784!
- Thanks to all

## draft-ietf-krb-wg-camellia-cts

- Now RFC 6803!
- Thanks to all

## draft-ietf-kitten-sasl-oauth (15 min)

- Jeffrey Hutzelman had comments during WGLC
  - The mechanism is not purporting actual security properties
  - Rev 10 was submitted to address some of these issues
  - Looking for feed-back on this update
- Same issues with:
  - SASL-SAML (RFC 6595)
  - SASL-OpenID (RFC 6616)
  - Do we address these security problems with errata?

# draft-ietf-kitten-kerberos-iana-registries (15 min)

- Revision 01
  - Specifies registry fields
  - Outstanding issues
    - Registry for application tag numbers?
      - draft-williams-kitten-krb5-extra-rt defines new PDUs but is not a complete module
    - Do transited encoding types need a registry?

# New Drafts (30 min)

- Proposed drafts as WG items
  - draft-williams-kitten-channel-bound-flag
    - Outstanding issues?
  - draft-williams-kitten-krb5-extra-rt
  - draft-williams-kitten-krb5-rcache-avoidance
  - draft-yu-kitten-kerberos-kdc-does-aliases
- Consensus to adopt?

# Open mic (5 min)

- Any comments/questions?

# GSS-Profile (15 min; time permitting)

- draft-williams-gss-profiles