Common Authentication Technology Next Generation (kitten)
Dallas, TX, USA – IETF 92

Ben Kaduk (kaduk@mit.edu)

Matt Miller (mamille2@cisco.com)

Shawn Emery (shawn.emery@oracle.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
- 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
- Any Birds of a Feather (BOF) session
- 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 participants
  - Agenda bashing
- WG document status (20 min)
- Kerberos PAD (10 min)
- Deprecating old Kerberos encryption types (10 min)
- Extra round trips in Kerberos (10 min)
- GSS-only Kerberos enctypes (10 min)
- PKCROSS (10 min)
- GSS generic naming attributes (10 min)
- Open Mic (5 min?)

WG Document Status

Approved by the IESG:

- draft-ietf-kitten-cammac
  - But, we recalled it. Security Considerations needs updating
- draft-ietf-kitten-gss-loop
  - Waiting for the RFC Editor

WG Document Status

Post-WGLC:

- draft-ietf-kitten-sasl-oauth
- draft-ietf-kitten-rfc4402bis
- draft-ietf-kitten-rfc6112bis
- draft-ietf-kitten-rfc5653bis

draft-ietf-kitten-sasl-oauth

- A set of SASL Mechanisms for OAuth
- Shepherd review found an old minor issue relating to ‘scope’ handling (see email).
- WGLC was otherwise successful, so this should be moving forward soon. (The shepherd writeup covers most of the 4.5-year history of the document; apologies to the relevant AD.)

draft-ietf-kitten-rfc4402bis

- A GSS PRF for Kerberos
- Part of the group of three “bis” documents’ WGLC
- No major issues
- Some minor editorial changes needed
- Needs someone to put out a new revision. Shawn?

draft-ietf-kitten-rfc6112bis

- Anonymity Support for Kerberos
- Part of the group of three “bis” documents’ WGLC
- Some edits needed
- A new WGLC may be needed depending on the nature of the edits.
- Need a volunteer to make edits -- Sam? Someone else?

draft-ietf-kitten-rfc5653bis

- Java GSS bindings update
- Part of the group of three “bis” documents’ WGLC
- The addition to GSSException performs the stated purpose and fills a need for that specific case (output token alongside error return)
- Issues raised with stream-based methods
  - With an output stream, an error token could be sent without API changes (probably none currently do)
  - Did the original authors of RFC 2853 properly understand the (non-)framing of GSS tokens?
  - Streams can be used correctly, but is it too complicated to realistically expect consumers to do so?
  - Proposal to mark as deprecated; further discussion needed

WG Document Status

WGLC queue:

- draft-ietf-kitten-aes-cts-hmac-sha2
- draft-ietf-kitten-pkinit-freshness (needs new revision)
- draft-ietf-kitten-gssapi-extensions-iana

WG Document Status

Documents not yet ready for WGLC:

- draft-ietf-kitten-sasl-saml-ec
- draft-ietf-kitten-iakerb
- draft-ietf-kitten-krb-auth-indicator
- draft-josefsson-kitten-gs2bis
- draft-ietf-kitten-channel-bound-flag
- draft-ietf-krb-wg-pkinit-alg-agility
- draft-ietf-kitten-kerberos-iana-registries

draft-ietf-kitten-sasl-saml-ec

- Scott has been very busy, so progress is slow
- A new version was posted in December
- Has anyone read it?

draft-ietf-kitten-iakerb

- Ben posted an update in October covering comments made in the previous WGLC
- Who has read it?
- Need a couple people to read and comment
- More edits may or may not be needed
- Will go into WGLC queue after some review is received

draft-ietf-kitten-krb-auth-indicator

- Authentication Indicator for Kerberos (string representing how the initial authentication was performed)
- First WG version back in February
- Who has read it? (Only 4 pages!)
- Do we want examples?
- May still need more updates

draft-josefsson-kitten-gs2bis

- GS2bis is needed to update the GS2 spec to allow mechanisms which do not provide channel binding and/or mutual authentication
- There are old comments in the archives which were not addressed.
- Someone needs to go through and find them all
- Alexey volunteered to make updates to address those comments.
- Do we still want to move this forward?

draft-ietf-kitten-channel-bound-flag

- Implementations of GSS channel bindings don't match the spec with respect to criticality of supplied bindings
- There is currently no way to incrementally upgrade an application protocol from no bindings to using them, without a flag day
- Has been expired for a while; is there still interest?
- Only relatively minor edits should be needed; any volunteers?

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

- Update PKINIT to remove structures tied to particular algorithms in favor of negotiation
- Expired in 2012
- Future-proofing that will be needed eventually
- Bill volunteered to be editor, but we dropped the ball on what changes were needed

draft-ietf-kitten-kerberos-iana-registries

- Tom has enlisted some help in verifying registries
- Seems a bit stalled?
- We promised to do this years ago…

Non-WG Document Status

Non-WG documents for consideration and old WG documents whose revival may be under consideration:

- draft-ietf-krb-wg-pad
- draft-kaduk-kitten-des-des-des-die-die-die
- draft-williams-kitten-krb5-extra-rt
- [GSS-only Kerberos enctypes; no draft yet]
- draft-williams-kitten-krb5-pkcross
- draft-williams-kitten-generic-naming-attributes
- draft-mccallum-kitten-krb-service-discovery
- draft-williams-kitten-impersonation-naming-attr

Non-WG Document Status

[presentations]

draft-mccallum-kitten-krb-service-discovery

- SRV records don’t scale well to new transport types and new services to discover (MS-KKDCP, proxies)
- Instead, make a single URI query and get back all types at once; another DNS query may be needed to resolve a hostname from the returned URI
- Converting clients to check the new record and realms to provide it will take time to transition
- How much interest in this work?

draft-williams-kitten-impersonation-naming-attr

- Naming extensions for S4U attributes
- Are we interested?

Open Mic

- Any comments/questions?