

GSS-API Next Generation (kitten-wg) Stockholm, Sweden – IETF 75

Charter Status

Tom Yu (tlyu@mit.edu)
Shawn Emery (shawn.emery@sun.com)

This working group is chartered to revise the GSSAPI v2 RFCs for the purpose of clarifying areas of ambiguity:

- o Use of channel bindings -- [draft-ietf-kitten-gssapi-channel-bindings](#)
- o Thread safety restrictions -- **TBD**
- o C language utilization clarifications and recommendations -- **TBD**
(e.g., type utilization, name spaces)
- o Guidelines for GSS-API mechanism designers -- **TBD**
- o Guidelines for GSS-API application protocol designers -- **TBD**

This working group is chartered to perform the following GSSAPI mechanism specification work:

- o Specify a GSSAPI v2/v3 Channel Conjunction Mechanism -- [draft-ietf-nfsv4-ccm-03 \(???\)](#)
- o Revise RFC 2478 (SPNEGO) to correct problems that make the specification unimplementable and to document the problems found in widely-deployed attempts to implement this spec. -- [RFC4178](#)
- o Update the GSSAPI Java Language Bindings to match actual implementation -- [draft-ietf-kitten-rfc2853bis-05](#)

This working group is chartered to perform the following new GSSAPI

Language Binding specification work:

- o Specify a language binding for C# -- [draft-ietf-kitten-gssapi-csharp-bindings-00](#) (???)

This working group is chartered to specify a non-backward compatible GSSAPI v3 including support for the following extensions:

- o Clarify the portable use of channel bindings and better specify channel bindings in a language-independent manner. -- [draft-ietf-kitten-gssapi-channel-bindings](#)
- o Specify thread safety extensions to allow multi-threaded applications to use GSSAPI -- **TBD**
- o Definitions of channel bindings for TLS, IPSec, SSH and other cryptographic channels based on work started in the NFSV4 working group. -- **TBD**
- o Define a GSSAPI extension to allow applications to store credentials. Discussions to be started based upon. -- [draft-ietf-kitten-gssapi-store-cred](#)
- o Extensions to solve problems posed by the Global Grid Forum's GSSAPI extensions document. -- [draft-ietf-kitten-gssapi-extensions-iana](#)

- o Extensions to deal with mechanism-specific extensibility in a multi-mechanism environment. -- [draft-ietf-kitten-extended-mech-inquiry](#)
- o Extend the GSS-API to support authorization by portable GSS applications while also supporting mechanisms that do not have a single canonical name for each authentication identity. -- [draft-ietf-kitten-gss-naming-05](#)
- o Specify a Domain-based GSS service principal name consisting of: service name, host name, and domain name for use by application services hosted across multiple servers. -- [draft-ietf-kitten-gssapi-domain-based-names](#)
- o Extensions to support stackable GSSAPI mechanisms. -- [draft-ietf-kitten-stackable-pseudo-mechs](#) (draft bound)
- o Define a Pseudo-Random Function for GSSAPI -- [draft-ietf-kitten-gssapi-prf](#)