KITTEN Misc: GSS-only enctypes

- AEAD cipher modes for RFC4121, but not Kerberos generally

- Two choices: share enctype number namespace with RFC3961, or... not

KITTEN Misc: GSS-only enctypes

- GCM, CCM, OCB – faster than RFC3962, **but**
  - AEAD cipher modes don't fit RFC3961
  - AEAD cipher modes have security issues with key re-use as in Kerberos long-term keys
  - AEAD cipher modes are faster than RFC3962
- AEAD ciphers modes do fit GSS per-msg token model

KITTEN Misc: Kerberos mech error recovery, rcache avoidance

draft-williams-kitten-krb5-extra-rt

- RFC4121 is a half or 1 round-trip mechanism
  - Errors are fatal
  - Some errors can notionally be recovered from

- Proposal (roughly; details matter, see I-D):
  - initiator indicates support for error recovery via ap-options
  - acceptor returns CONTINUE_NEEDED on such errors
  - Initiator recovers, sends another AP-REQ token

KITTEN Misc: Kerberos mech error recovery, rcache avoidance

- Recoverable errors:
  - User2user!
  - Wrong kvno
  - Expired ticket (KRB-ERROR can be protected)
  - Clock skew (KRB-ERROR can be protected)
  - Ticket not yet valid, ...
- Replay cache avoidance: one more PDU/sec context token

KITTEN Misc: PKCROSS

draft-williams-kitten-krb5-pkcross

- Manual x-realm keying is a terrible thing
- It's manual (operators learn the keys)
- It doesn't scale

KITTEN Misc: PKCROSS

draft-williams-kitten-krb5-pkcross

- hx509 (or replacement) + bits of PKINIT + DANE we can build PKCROSS
  - Client gets cert from hx509, uses it as PKINIT cert at target
  - TGSes can also setup temporary xrealm trusts to support clients that don't do PKCROSS, and as a significant optimization
  - DANE stapling for target realm authentication

KITTEN Misc: Name attributes

draft-williams-kitten-generic-naming-attributes

- Some useful name attributes that could be exposed by GSS implementations, with generic and Kerberos-specific forms
  - Issuer of peer name (CA, realm)
  - Transit/validation path
  - “components” (service name, hostname, username, …)