GS2: Bridge between SASL and GSS-API

- Info: http://josefsson.org/sasl-gs2/
  - Questions? simon@josefsson.org

- Draft -02 posted Jul-06.
  - WGLC during 31 Aug – 18 Sep.
- Draft -03 posted Nov-06
  - Solves several WGLC issues.

- Please verify that -03 is complete...
  - ...except known open issues on next slides.
GS2: Bridge between SASL and GSS-API

• Open Issue 1/3: Support for GSS-API credentials/mechanisms without integrity
  – Feature request that came up during WGLC.
  – Vulnerable to MITM unless we require TLS.
  – We can't support non-integrity capable credentials until KITTEN defines new APIs.
  – Complicates protocol and implementations
    • Creeping featurism, no IETF standard use-cases.
    • Alternative: Specify another SASL family GS0 for these mechanisms?

• How to resolve:
  – Option 1: Publish -02 now, revise GS2 or do GS0 later.
  – Option 2: Revise GS2 now (volunteers?).
GS2: Bridge between SASL and GSS-API

• Open issue 2/3: Channel binding documents
  - GS2 reference d-w-on-channel-binding-00.
  - TLS channel bindings are specified in draft-altman-tls-channel-bindings-00.
  - Not sufficient to be able to implement GS2 today.
    • Underspecified channel binding syntax for TLS.
    • Reason for failure to implement GS2 in GNU SASL.

• How to resolve:
  - Option 1: Reference draft-altman-tls-channel-bindings in GS2 and explain how to use it explicitly.
  - Option 2: Improve other drafts, possibly writing a new document to describe how channel bindings are used in GS2 or SASL in general.
GS2: Bridge between SASL and GSS-API

Open issue 3/3: Compute Kerberos V5 GS2 mech name
   - Need two independent computations
     • I have one so far, noticed several ways to go wrong, not confident of my result.
   - This is used only in the example section.
     • However, WILL be hard-coded in implementations to avoid having to implement B32/SHA1/DER.
       – B32(TEN(SHA1(DER(KRB5-OID)))))
         • B32 – Base32 encoding
         • TEN – First ten bytes
         • SHA1 – SHA.1 hash
         • DER – ASN.1 encoding
         • KRB5-OID – from RFC 1964
   - How to resolve: Volunteer(s) needed