Background

- Will obsolete RFC 3920 ("XMPP Core")
- Many errata, corrections, and clarifications
- Lots of implementation experience!
- Updates to TLS (5246) and SASL (4422)
- More detailed security considerations
- Other non-material changes
Material Changes

• Include ‘from’ and ‘to’ on most stream headers
• Moved server dialback to XEP-0220 @ xmpp.org
• XML processing
  • Loosened requirements regarding predefined entities that are not escaped in XML
  • Comments, PIs, and DTDs are still forbidden
  • Namespace well-formedness is optional
Open Issues

• Internationalization
• Certificate generation and handling
• Mandatory-to-implement SASL mechanisms
• Client resource binding
• Formal representation
• Other?
Internationalization

- 3920 has dependencies on IDNA (3490) and stringprep (3454) for XMPP addresses (“JIDs”), as does bis-00
- IDNAbis work is ongoing and any stringprep changes are on hold
- What is the best path forward for i18n of XMPP addresses?
Certificates

- Client certs: unchanged
- Server certs
  - 3920: dNSName then XmppAddr (domain name allowed in CN)
  - bis: SRVName (4985), then dNSName, then XmppAddr (CN only for friendly name)
SASL Mechanisms

- 3920: DIGEST-MD5 for confidentiality and authentication
- bis:
  - DIGEST-MD5 to historic by SASL WG
  - currently recommend TLS + SASL PLAIN
- add SCRAM? (draft-ietf-sasl-scram, in WGLC)
Resource Binding

- Client needs resource identifier for routing (full JID = user@domain/foo)
- 3920: client can specify but server can override (or client requests server generation)
- bis-00: can bind multiple resources
- bis-01: consensus to remove multi-bind?
Formal Representation

• 3920: uses W3C XML Schema, but the schemas are non-normative

• bis: Add Relax NG?
  • In addition to W3C schema?
  • Instead of W3C schema?