

# TLS Re-Charter

# Focus of Updates

- Improve TLS usage in emerging protocols
  - TLS as an AKE
  - Exported Authenticators
  - Extensibility
  - Size
- Improve Security, Privacy and Deployability
  - Encrypt more of client hello
  - Fingerprinting mitigations
  - Padding
- Maintain Current and Previous Versions
  - Best practices
  - Deprecation