Agenda

• Introduction & house-keeping
• TLS 1.3 plans & progress
• Driver interface code-gen (discuss #5067)
Introduction & House-keeping

• Planned times & cadence
  • Every two weeks
  • Alternate US and Asia friendly times (10am and 4:30pm UK time)
    – i.e. 10am meeting every four weeks, and 4:30 meeting every four weeks, two weeks apart
  • Calendar available on trustedfirmware.org

• Content
  • Agenda & call for topics to be published during the preceding week
    – Email to mbedtls-list and mbedtls-announce
    – Please raise any topics you would like to discuss

  • Typical content
    – Engineering-driven technical discussion
    – Share Mbed TLS plans & time-lines
    – Understand community asks & priorities

• All welcome to attend

• Afterwards
  • Slides & recording available via trustedfirmware.org
Use PSA Cryptography API
- TLS 1.2 also
- PSA driver interface

Message Processing Stack
- Handshake messages (de)fragmentation

TLS 1.3 MVP
- TLS 1.3 client
- Ephemeral key establishment
- Server Authentication

TLS 1.3 server
- Negative testing

Pre-Shared Keys
- PSK + Ephemeral
- 0-RTT

PQC key agreement

Using TLS to Secure QUIC

For more info, please see
Thank You
Danke
Merci
Merci
Monkeys
Kittos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה