

A photograph showing a group of six people (three men and three women) gathered around a whiteboard in a meeting room. They are looking at a tablet device held by one of the men. The whiteboard has some handwritten notes and diagrams. The scene is lit from above, creating strong shadows on the floor.

arm

# Mbed TLS Tech Forum

Dave Rodgman  
2021-10-25

# 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](https://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](https://trustedfirmware.org)

## Use PSA Cryptography API

TLS 1.2 also

PSA driver interface

## Message Processing Stack

Handshake messages  
(de)fragmentation

## TLS 1.3 server

Negative testing

## TLS 1.3 MVP

TLS 1.3 client

Ephemeral key establishment

Server Authentication

## PQC key agreement

## Pre-Shared Keys

PSK + Ephemeral

0-RTT

## Using TLS to Secure QUIC

arm

Thank You

Danke  
Merci

謝謝

ありがとう

Gracias

Kiitos

감사합니다

ধন্যবাদ

شَكْرًا

ଧନ୍ୟବାଦ

תודה