

Extensions to TLS FATT Process (draft-usama-tls-fatt-extension)

Muhammad Usama Sardar

July 23, 2025



Motivation and Main Idea

- Motivation
 - **Small** formal methods community
 - **Steep** learning curve for formal methods tools
 - **Sustainability** of FATT process

Motivation and Main Idea

- Motivation
 - **Small** formal methods community
 - **Steep** learning curve for formal methods tools
 - **Sustainability** of FATT process

- Necessary components of draft *before* adoption
 - **Threat model**
 - **Informal security goals**
 - **Protocol diagram** (similar to the *Protocol Model* in RFC4101)