RATS WG
Reference Interaction Models

Henk Birkholz <henk.birkholz@ietf.contact>

IETF120 Vancouver, 23rd July
Language about TPM Requirements


- OLD: prescriptive about dedicated TPMS
- NEW: allows for equivalent hardware, including TPM functions baked into "bigger silicon" or equivalent hardware that adheres to TCG TPM specifications
Last Remaining Review Comments Addressed


• Added clarification on nonce use
• Updated text & ref to epoch markers
• Clarified the optional nature of Claim Selection by Challenger
• Relabeled Authentication Secret ID to Attestation Key ID
• Polished wording on Attestation Key Knowledge (spoiler: the Challenger/Verifier might not have a clue)
WGLC


• More eyes to move it across the finish line?
• The I-D grew in complexity over time
• A first WGLC could be useful to assess alignment with other RATS RFCs and I-Ds
• What does the WG think?