DTLS Profile

IETF#91

Hannes Tschofenig

Status

- Latest version: https://tools.ietf.org/html/draft-ietf-dice-profile-05
- Addressed review comments from Michael St. Johns
- Changes included:
  - Updated references
  - Improved wording regarding certificate depth,
  - Clarification that SHA-256 implementation is needed due to PRF construction, PSK identity exchange and identity hint exchange.
  - Added reference to RFC 7228 for terminology.
- Diff: https://tools.ietf.org/rfcdiff?url2=draft-ietf-dice-profile-05.txt
- Proposal to start WGLC to finalize the work.