The following full text is a publisher's version.

For additional information about this publication click this link.
http://hdl.handle.net/2066/34748

Please be advised that this information was generated on 2017-11-03 and may be subject to change.
FORMALIZING SHIM6
AN IETF PROPOSED INTERNET STANDARD IN UPPAAL
Matthijs Mekking1, Wouter Wijngaards1, Frits Vaandrager2, Theo Schouten2
1 Foundation NLnet Labs
2 Institute for Computing and Information Sciences, Radboud University Nijmegen

Matthijs@nlnetlabs.nl
wmecking@science.ru.nl

Revealed incorrectness upon receiving pay-load in I2-SENT or I2BIS-SENT.
Revealed possible deadlock with optional re-transmitting I2 / I2bis messages.
Clarified confusion about responder nonce.
Revealed several other ambiguities, omissions and inconsistencies.
Acknowledged by SHIM6 draft authors.
Will be incorporated in new IETF proposal.

Future Work

UPPAAL:
Improve model to verify on scale.
Add failure detection and exploration.
Extend UPPAAL verifier language.
Indicate model state space.

SHIM6:
Implementations.
Add HBA and CGA, Context Forking.
INTEROP test.
Traffic engineering issues.

UPPAAL:
http://www.uppaal.com