WiP: Towards Formal Specification of Attestation Frameworks for Confidential Computing

Muhammad Usama Sardar[1], Thomas Fossati[2], Hannes Tschofenig[3] and Simon Frost[4]

[1]TU Dresden, Germany

[2]Linaro, Lausanne, Switzerland

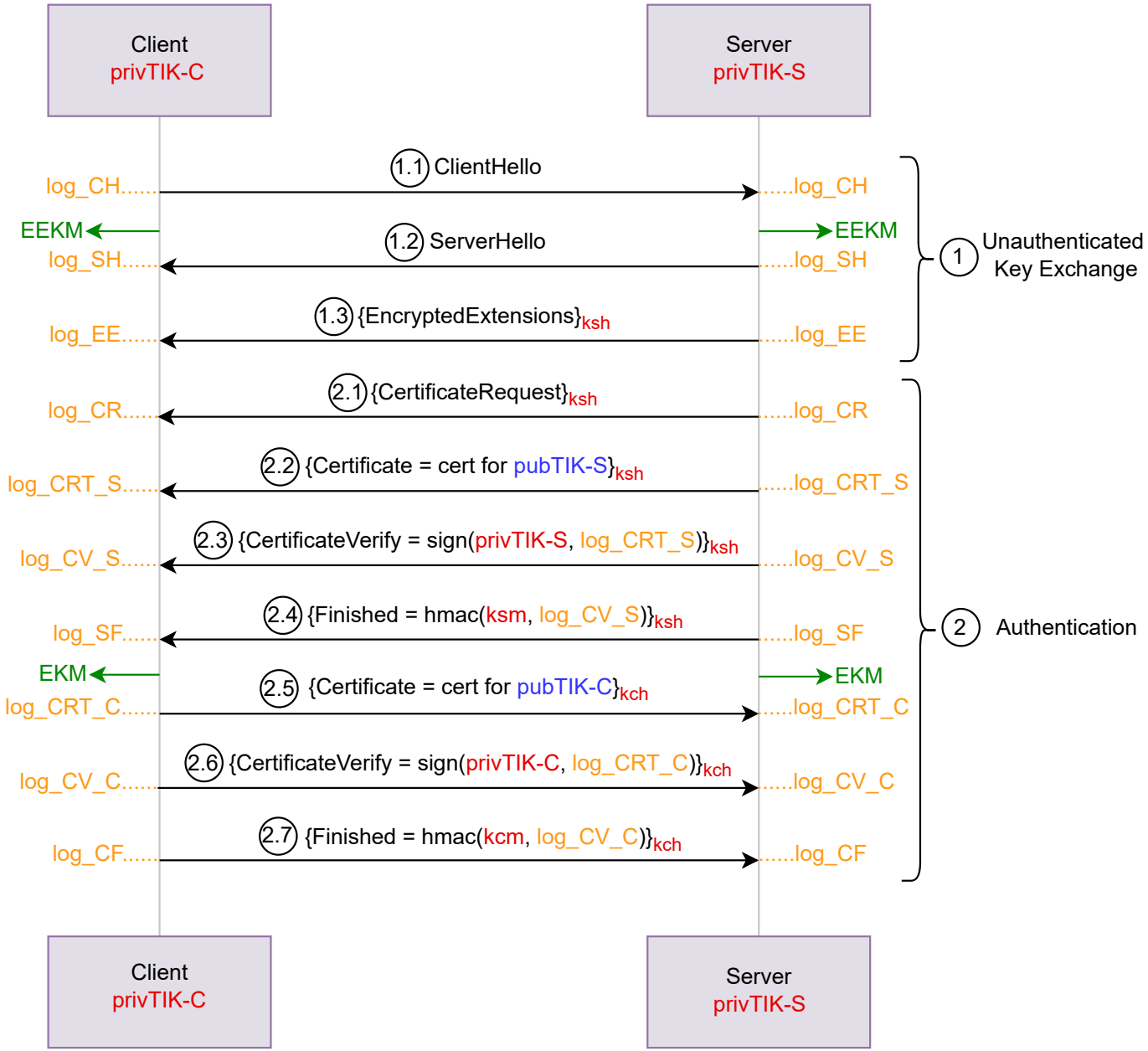
[3]University of Applied Sciences Bonn-Rhein-Sieg and Siemens, Germany

[4]Arm, Cambridge, UK

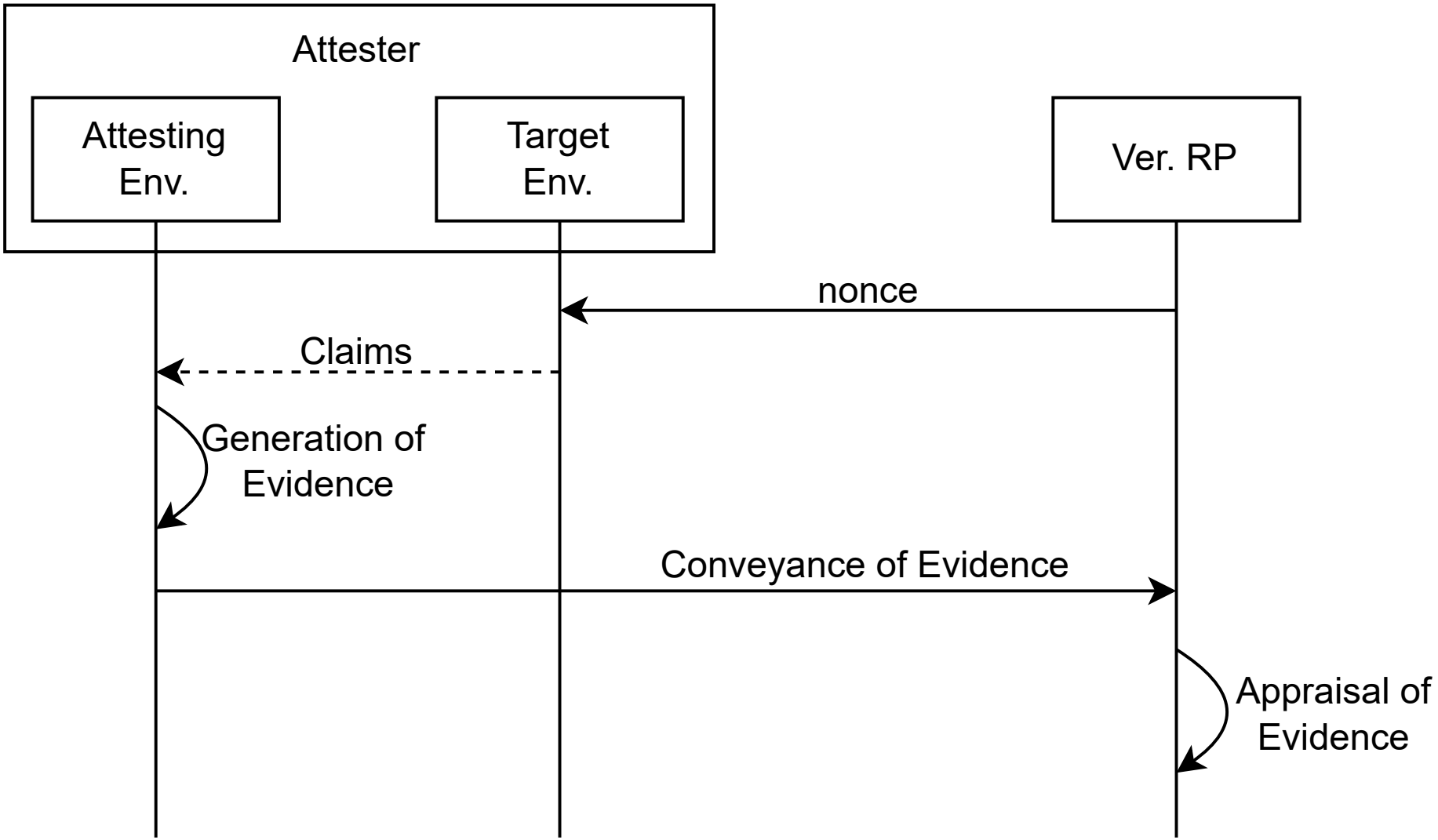
November 2, 2024

Outline

Network Security: TLS



Endpoint Security: Remote Attestation for CC

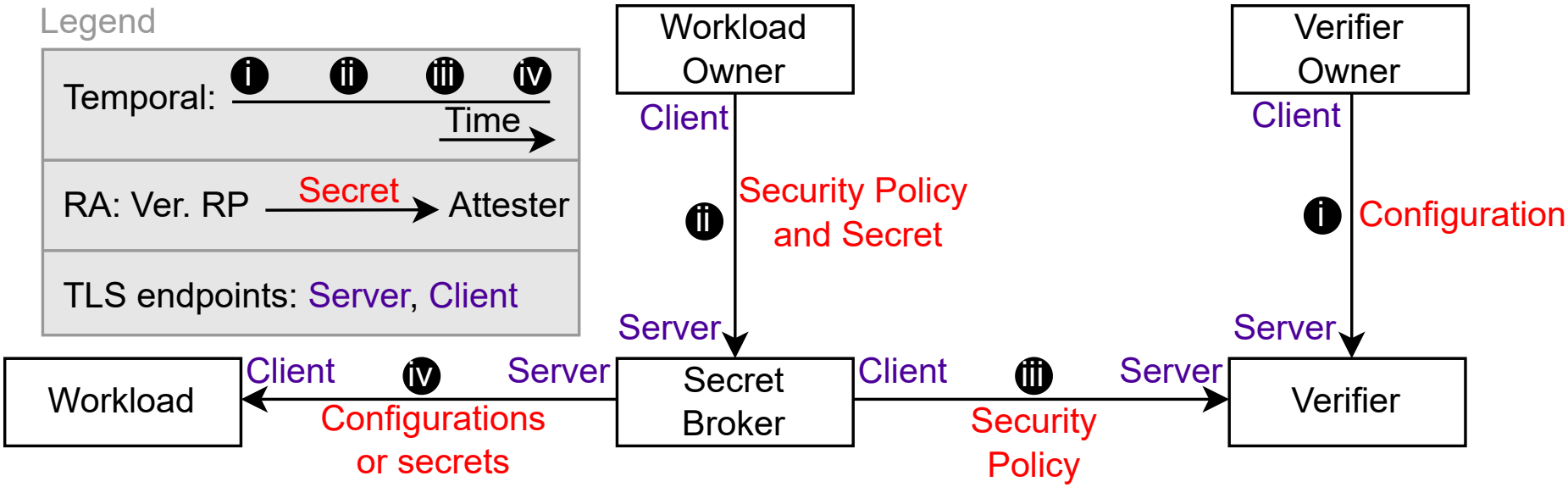


Motivation


TDX
DOWN
Single-Stepping and Instruction Counting Attacks against Intel TDX
TDXdown presents two attacks on TDX's single-stepping countermeasure and uses them to recover ECDSA keys via a new weakness in nonce generation of OpenSSL and wolfSSL.

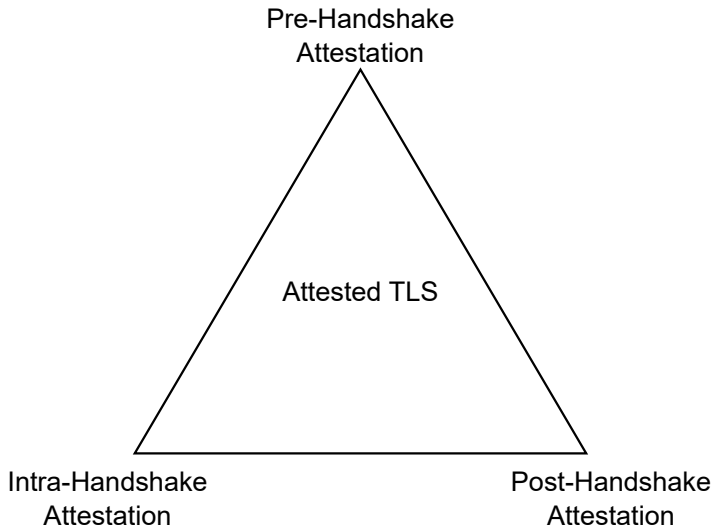
Outline

Proposed Generic Architecture

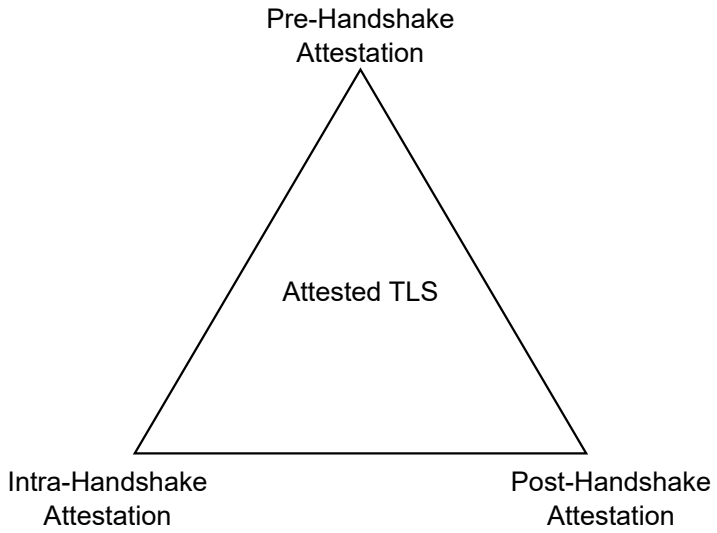


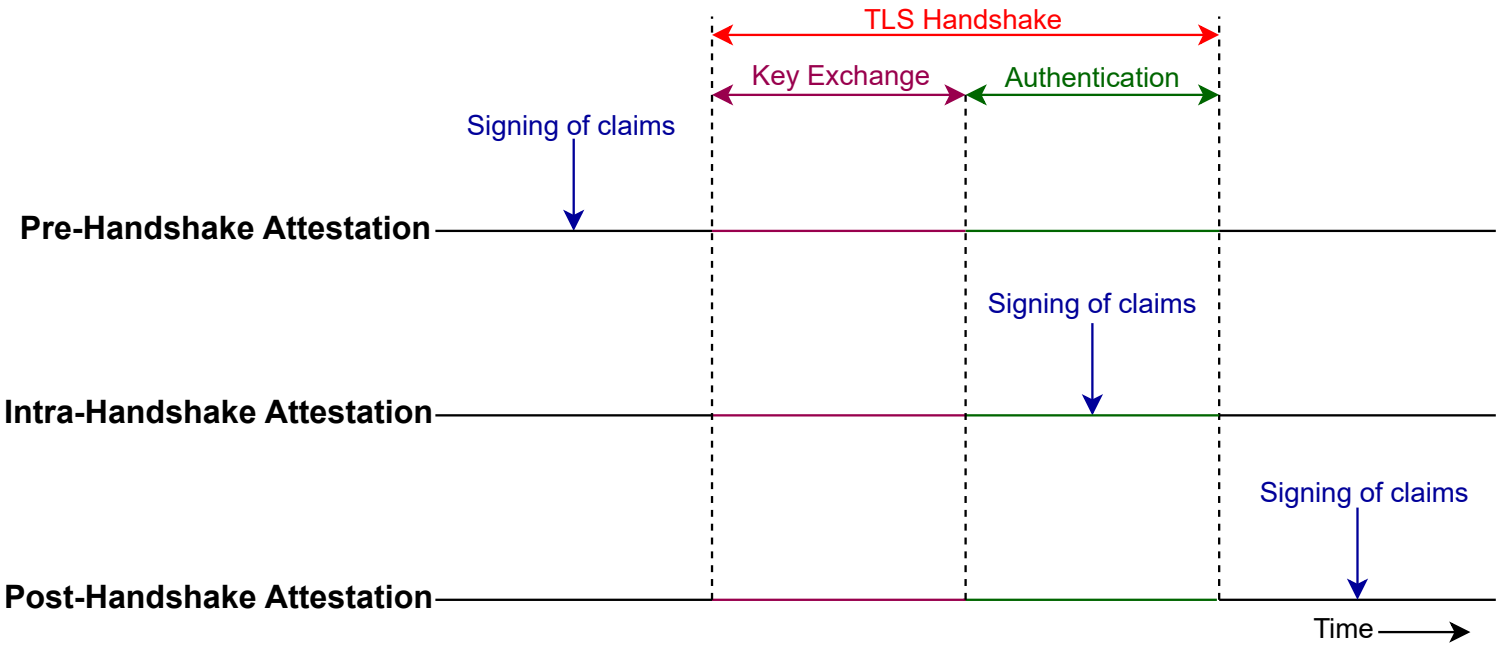
- Stages i and ii are unspecified for all solutions!

Design Options

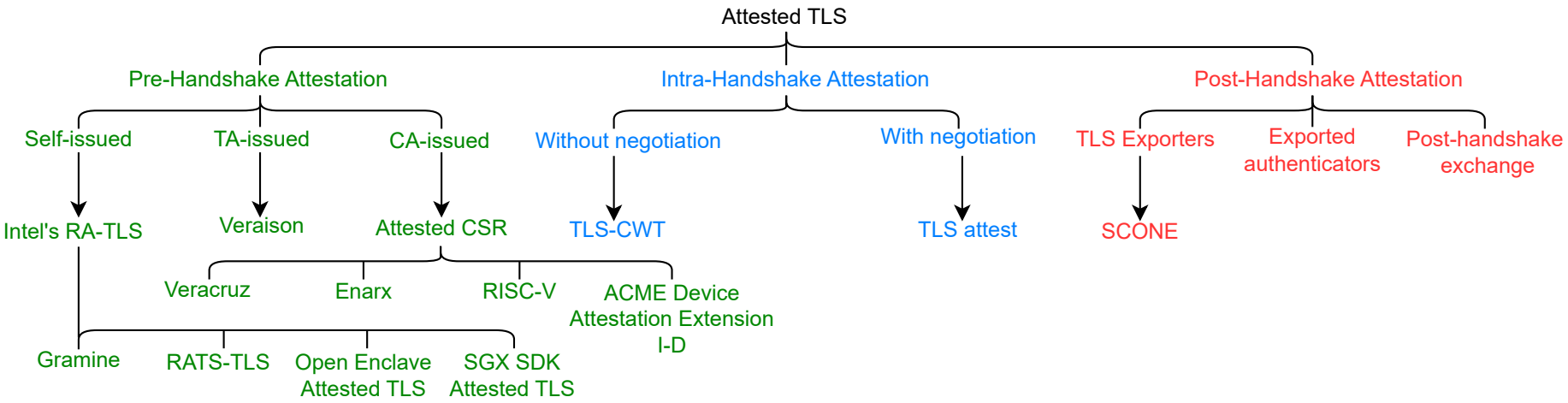


Design Options





Design Space for Attested TLS



(Typical) Comparison/Tradeoffs

Property	**Pre-handshake**	**Intra-handshake**	**Post-handshake**
Modification	TA/CA	TLS	Application
Replay protection	×	✓	Possible
Impact on connection establishment latency	Medium ($t_{hs} + t_a$)	High ($t_{hs} + t_g + t_a$)	Low (t_{hs})
Effective connection establishment latency	Low	Low	High ($\geqslant$0.5RTT)

- t_{hs} = Time for TLS handshake (without attestation)
- t_g = Time for generation of evidence
- t_a = Time for appraisal of evidence
- WiP
  - Usability/Ease of use
  - Complexity of implementation/formal verification
- Discussion: any other property?

Outline

Summary

- Design choices: pre-/intra-/post- HS attestation

Summary

- Design choices: pre-/intra-/post- HS attestation
- Interlink between arch. specs and protocol specs

Summary

- Design choices: pre-/intra-/post- HS attestation
- Interlink between arch. specs and protocol specs
- Underspecified = NOT trustworthy!

Summary

- Design choices: pre-/intra-/post- HS attestation
- Interlink between arch. specs and protocol specs
- Underspecified = NOT trustworthy!
- The process of formal specification (even without verification) is very valuable!

Summary

- Design choices: pre-/intra-/post- HS attestation
- Interlink between arch. specs and protocol specs
- Underspecified = NOT trustworthy!
- The process of formal specification (even without verification) is very valuable!
- Open Questions

Summary

- Design choices: pre-/intra-/post- HS attestation
- Interlink between arch. specs and protocol specs
- Underspecified = NOT trustworthy!
- The process of formal specification (even without verification) is very valuable!
- Open Questions
  - How to efficiently and automatically verify underspecified systems?

Summary

- Design choices: pre-/intra-/post- HS attestation
- Interlink between arch. specs and protocol specs
- Underspecified = NOT trustworthy!
- The process of formal specification (even without verification) is very valuable!
- Open Questions
  - How to efficiently and automatically verify underspecified systems?
  - How to discover missing specs automatically?