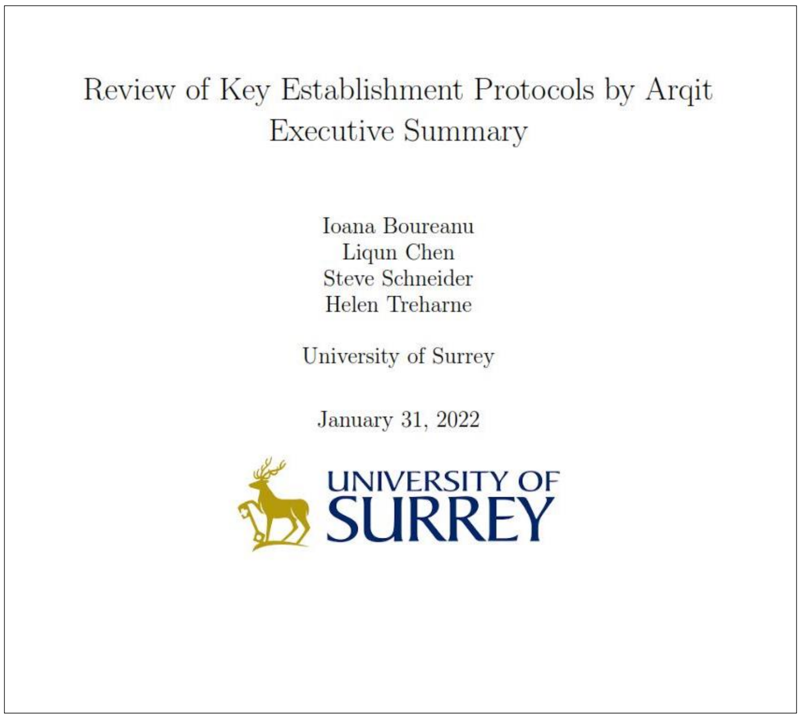
Independent Assurance Review on Arqit's Technology



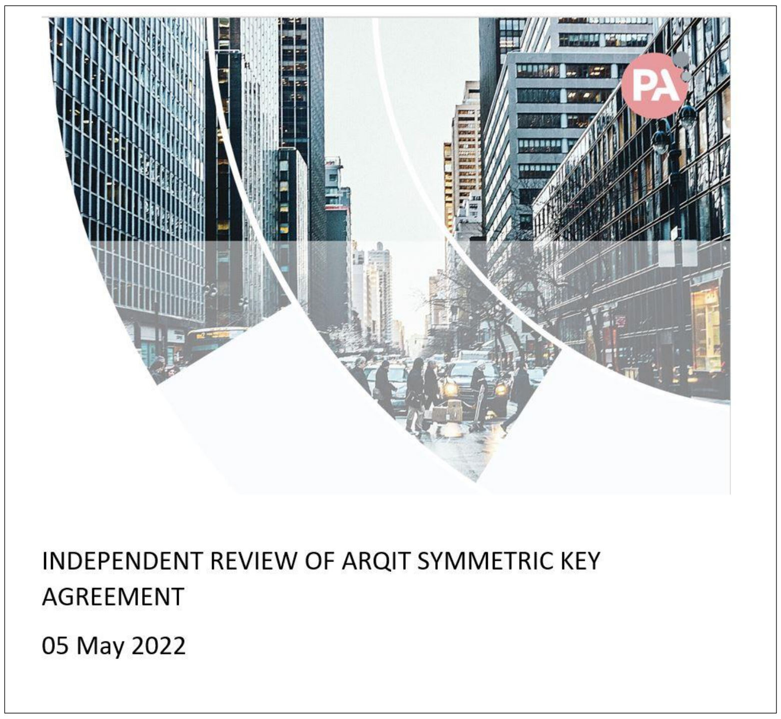
Review of Key Establishment Protocols by Arqit
Executive Summary

Ioana Boureanu
Liqun Chen
Steve Schneider
Helen Treharne

University of Surrey

January 31, 2022

UNIVERSITY OF SURREY



INDEPENDENT REVIEW OF ARQIT SYMMETRIC KEY AGREEMENT

05 May 2022

University of Surrey's Review of Key Establishment Protocols by Arqit - Executive Summary

The assurance study has been based on a set of information provided by Arqit and interviews with the Surrey Centre for Cybersecurity at the University of Surrey.

Arqit's Protocol Framework specifications relate to Arqit's solution for "quantum safe" enterprise communications. The formal mathematical models of the Protocol Framework have been tested with a recognised unbounded symbolic protocol prover, the Tamarin prover. In our view Tamarin is the industry preferred tool, having a recognised pedigree in verifying the robustness of the cryptographic protocol that provides communication security on all modern websites.

The formal tests have successfully shown that the protocols uphold their desired security properties in the symbolic model, and against our best estimation of its threat model.

The University of Surrey is accredited as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR) by the British government. It plays an important role in helping to make the UK government, businesses and consumers more resilient to cyber-attacks.

Professor Steve Schneider, Director of the Surrey Centre for Cyber Security, said "We were pleased to verify the Security Proof of Arqit's design which we found to be excellent. The technology represents a significant advance in secure communications".

PA Consulting's Independent Review of Arqit Symmetric Key Agreement

Executive Summary

- PA Consulting has been engaged by Arqit to provide independent technical review on three cryptographic key establishment protocols intended to connect computing devices to a Cloud service. We refer to these as Arqit's Protocol Framework.
- The Tamarin proof reflects security by design principles and demonstrates the robustness of the protocols' mathematics.
- The findings give us confidence that the core protocols defining the building block for security of computing device-to-Cloud connectivity will meet their stated security goals.

PA's work builds upon a technical review by University of Surrey which utilised a well-established Tamarin cryptographical modelling tool to validate the mathematical underpinnings of two foundational key establishment protocols.

Arqit customers may access the PA Consulting report. To do so, please discuss with your Arqit account manager.