

Ref. No: 6782/2024-NÚKIB-E/610

Prague, September 3, 2024

### **Letter of Support to the “Position Paper on Quantum Key Distribution”**

On behalf of the National Cyber and Information Security Agency (NÚKIB) of the Czech Republic, we would like to declare our support for the message and content of the “Position paper on Quantum Key Distribution”, published jointly on January 26, 2024 by the French Cybersecurity Agency (ANSSI), the German Federal Office for Information Security (BSI), the Netherlands National Communications Security Agency (NLNCSA), and the Swedish National Communications Security Authority, Swedish Armed Forces.

This position paper highlights current and inherent limitations on quantum key distribution (QKD), especially from the security perspective. NÚKIB agrees with the conclusions that further research on QKD is desirable so that some of its current limitations may be overcome, and that the technology itself may be useful in other areas. Nonetheless, NÚKIB also shares the concerns expressed in the paper and supports the main statement that “in light of the urgent need to stop relying only on quantum-vulnerable public-key cryptography for key establishment, the clear priorities should therefore be the migration to post-quantum cryptography and/or the adoption of symmetric keying”.

Yours faithfully

Lukáš Kintr  
Director  
National Cyber and Information Security Agency