Appendix 11
Further Research Needs for QKD, RKD, MKD

Because the diverse R&D activities currently underway at various research centers worldwide or planned for the near future are largely confidential and therefore cannot be disclosed, this work package has been kept very general and viewed from the perspective of the state of the art.

A detailed description would not be possible at all, particularly for QKD, by the team of authors, who do not conduct research in this field.

1 QKD

Of the three technologies described—QKD, RKD, and MKD—QKD has by far the greatest need for further research. QKD must, above all, significantly increase key rates, particularly over longer distances; the technology must become significantly more cost-effective; dangerous side-channel attacks must be better defended against; the stability of individual, particularly error-prone components must be improved; and the trusted nodes required for longer distances still have extensive potential for improvement.

There is also a significant need for research regarding the integration of satellites. Among these research activities, the greatest need lies primarily in entanglement technology, which, while the most fascinating and secure, is also the most complex and the most recent technology.

This technology is also particularly complex when it comes to trusted nodes. Of the three QKD technologies described, entanglement technology is the only one in which the non-deterministic random number generator is inherently integrated into the technology, is 100% secure according to the laws of physics, and both communication parties use the same terminal—two very important characteristics in practice. Therefore, it would be particularly important for research on entanglement

technology in the coming years to be sufficiently extensive and successful in addressing the research needs outlined above.

Another key aspect of QKD is the great need for standardization, which is still in its infancy.

2 RKD

In contrast, RKD is a significantly older and simpler technology. Measurements during radio transmission in these frequency ranges have been common and proven for over a century, and there are many SDRs (Software-Defined Radios), including affordable ones, available on the market. The body of scientific literature on RKD is now very extensive. In RKD, the research needs lie, on the one hand, in determining the final key from the measured values and, on the other hand, in the artificial generation of motion so that usable measurements can be obtained even when stationary or with little movement. The available components already allow to develop and produce excellent and cost-effective devices today, as demonstrated by the RKD device from insitu. There is also no standardization for RKD yet. However, due to the possibility of using a wide range of industry-standard products on the market, standardization here is much easier and faster to implement.

There is a significant need for research regarding the use of RKD in conjunction with satellites. This involves key exchange between a ground station and a satellite to enable highly secure communication between satellites and Earth. In contrast, the use of RKD between two ground stations via a satellite does not currently appear to be a practical option.

3 MKD

The situation is simplest with MKD. Here, research focuses on the non-deterministic random number generator. Higher speed and simpler verification of true randomness would be desirable here.

Research on MKD-capable storage media is currently being conducted without the involvement of MKD, because manufacturers of secure SSDs have a strong interest in increasing storage capacity and improving security on their own initiative. For HSMs, there is little need for further improvements, particularly in the context of MKD.

The logistics processes required for distributing cryptographic keys can still be slightly improved, and there may be a need for research in this area.

Standardization for MKD is very well established due to the existence of good industry standards.