Appendix 12
Deployment Analysis of QKD, RKD, and MKD

This chapter analyzes which methods can be fully developed and deployed most quickly in practice to provide seamless protection. Since products and solutions already exist for all the technologies discussed and are being used in practice, at least in pilot projects, this appendix is not concerned with development and rapid deployment, but rather with simplicity.

1 QKD

For QKD to be deployed, at a minimum, QKD endpoints, encryption units, and the connection infrastructure are required.

The encryption unit can take various forms, e.g., as a hardware box that receives the cryptographic keys from the QKD terminal and the data to be encrypted from a terminal. However, it can also be part of the terminal where the data to be encrypted is located.

A wide variety of QKD terminals are available on the market (see Chapter**Fehler! Verweisquelle konnte nicht gefunden werden.**). However, all QKD terminals must support the same QKD technology and, due to the still very limited standardization, usually must also come from the same manufacturer. This means that if a manufacturer is changed in the future—because it is no longer desired due to performance data, price, error susceptibility, etc.—all QKD endpoints usually have to be replaced. With a large number of existing QKD terminals, such a change represents a very significant investment due to the high cost per QKD terminal (over $100,000 each).

The connection infrastructure also represents a significant investment due to the required fiber-optic cables and, above all, the trusted nodes for distances exceeding

approximately 150 km. For very long distances, special satellites are required, which are extremely expensive and require complex ground stations. This connection infrastructure can usually be reused when switching QKD terminal manufacturers. However, setting up this infrastructure can be very time-consuming in addition to being costly, and the infrastructure is highly sensitive to external influences.

The trusted nodes and satellites are particularly complex components of the connection infrastructure. This is primarily due to security concerns, as the satellites typically act as a man-in-the-middle in some of the technologies described. Securing the trusted node also poses a major challenge, as practical operation over an extended period involves maintenance tasks that are only possible to a very limited extent on a trusted node.

Overall, the use of QKD entails very high costs, a very high degree of dependence on the manufacturer, and significant challenges in practical operation.

2 RKD

For RKD, at a minimum, RKD end devices and encryption units are required; communication takes place via radio.

The RKD terminal is a small, compact, and very cost-effective device. Currently, there is only one provider of RKD terminals (see Chapter 4). All RKD end devices must support the same RKD technology, which, however, does not necessarily pose a problem in practice because products from the global market are used here and the selection is not very large. Furthermore, RKD devices are so inexpensive that even a necessary change of manufacturer would not represent a significant investment in terms of cost.

The encryption unit can take various forms, e.g., as a hardware box that receives the cryptographic keys from the RKD terminal and the data to be encrypted from a terminal. However, it can also be part of the terminal where the data to be encrypted is located.

Because of the wireless transmission, no special connection infrastructure is required.

There are currently no RKD terminals on the market capable of long-distance communication via satellite, and no scientific research has yet been conducted in this area. At least one known research project has been active in the field of communication between satellites and RKD terminals on Earth.

3 MKD

For MKD, at a minimum, non-deterministic random number generators, MKD-capable storage media (which can also be smart cards if a one-time pad is not used), and encryption units are required. Key exchange occurs through the physical transport of the MKD-capable storage media. The encryption units can also be integrated directly into the terminal

The selection of suitable random number generators and MKD-capable storage media on the global market is extensive. They all operate with standardized interfaces (USB, SATA, PCIe), meaning switching manufacturers is straightforward. Software adjustments or a change in driver software may be necessary.

The encryption unit can take various forms, e.g., as an HSM that receives the cryptographic keys from the MKD-capable storage medium and the data to be encrypted from an end device. However, it can also be part of the end device where the data to be encrypted is located.

No connection infrastructure is required because key transport occurs physically via the storage media. To implement key transport, the use of suitable software is recommended.