7. Conclusion

The investigation of the Matter communication standard with regard to security aspects carried out as part of the project shows that Matter is able to cleverly combine the two standards (Wi-Fi and Bluetooth) with one another. The simple use of Bluetooth provides a user-friendly method of commissioning of new devices into a Matter network, while the communication of existing connections occurs exclusively via Wi-Fi. Since Bluetooth is automatically switched off after the commissioning process, the respective strengths of the standards can be applied in a targeted manner.

The sniffing attacks on Wi-Fi and Bluetooth carried out in the test show that this procedure is also necessary, since capturing the packets under Bluetooth was many times easier and more successful than that of Wi-Fi. It can also be confirmed that some considerations have been made with regard to security aspects of Bluetooth, as can be seen, for example, in the randomisation of the MAC address and the encryption of the communication. However, the sniffing attacks carried out via Bluetooth show that it is possible to record the data exchange when Matter devices are commissioned.

Furthermore, it can be confirmed that Matter supports the latest security standards of Wi-Fi, such as WPA3. The data integrity could also not be attacked in the experiments, which prevented a man-in-the-middle attack as part of a replay attack. However, it had to be determined that basic security functions under the older security protocol WPA2 were insufficiently taken into account in the tested version 1.1 of Matter. So it is not apparent that Wi-Fi's 802.11w security feature is built into and supports Matter. It follows that the current version of Matter is susceptible to de-authentication attacks that are easy to carry out, and communication in a Matter network can therefore be significantly impaired by such attacks. This also amplifies the threats regarding downgrading attacks, causing malicious actions in this context can lead to greater damage.

It can therefore finally be stated with regard to the research question that Matter in the current version is not able to overcome all the vulnerabilities of the standards used for Matter. Although a large number of security aspects are taken into account under Matter, not all proven security functions are used. In addition, Matter is largely based on the recommended procedures of the standards used and uses the security features, but does not expand them further, so that significant reinventions of security aspects could not be found within the framework of the project. It should be noted, however, that Matter is in a published version at

the time the project has been carried out, but it is still relatively early in its development cycle. During the period of this project, it could be observed that intensive work continued on the Matter Repository, so that there is hope that the security of the standard will also be significantly further developed and improved in the further development process of Matter. Whether or not Matter will be the communication standard in the IoT Smart Home area, which makes the multitude of standards currently in use redundant, remains to be seen in the future. However, the mitigation of possible vulnerabilities in the standard, as well as those identified in this project, will be a key factor in Matter establishing itself in the market and user acceptance of this standard.

The experiments carried out in this project form an initial basis for assessing the quality of Matter's security. However, some suggestions for further work can be generated in relation to Matter and as a product of this project. In this project, the Thread communication standard, which is also supported by Matter, was not examined for possible security gaps. Possible vulnerabilities with regard to communication through interoperability between Wi-Fi and thread also represent an interesting basis for further research.

Furthermore, the results of the Bluetooth sniffing of this project offer further research potential in relation to the security of the encryption of the data packets and possible threats to decrypt them. In addition, the discovered threat of possible vulnerabilities related to WPA2 and downgrading attacks on Matter devices is also an item that should be investigated in depth.

Finally, only freshly flashed and non-certified Matter devices were used as part of this project. Due to the observation of the different security features of the hub devices, these also offer further research potential, since on the one hand the question can be asked how secure the certificates are in terms of manipulation. On the other hand, investigating the potential threat of reselling hacked certified Matter devices to secondary consumers offers another comprehensive research spectrum that should be investigated.