Device security

- 1.1 What does "root of trust" mean? What attacks are prevented by using a "root of trust"?
- 1.2 What is/are the cryptographic primitive(s) used to create a "root of trust"? Explain its/their purpose(s).
- 1.3 What properties does the root hash provide?
- 1.4 Describe the steps needed to perform a firmware update.
- 1.5 Give two/three benefits for using a trusted environment? Explain these benefits from a security point of view.