14 Topical Issues (RKH)

(*a*) Describe the operating principles of RFID systems based on capacitive, inductive and backscatter coupling. Give typical operating ranges and at least one example application for each. [9 marks]

(*b*) Electronic passports contain RFID chips to permit electronic transfer of biometric data to a reader. The systems in use today use remote-coupling with an operating frequency of 13.56 MHz. The full communication protocol varies, but every transmission from the passport is prefaced with a numeric identifier (UID).

(*i*) The first implementations used a static UID unique to each passport, whilst later implementations generated a new pseudo-random UID for each round of communications. Outline the risks and practicalities of each approach. [3 marks]

(*ii*) Biometric data are usually encrypted when sent between reader and tag using a protocol known as Basic Access Control (BAC). The shared session key is generated solely from the owner's passport number (9 digits), passport expiry date and date of birth. These data must be read *optically* by swiping the passport through a desktop device before proceeding. Comment on the security of this system and the choice of 13.56 MHz RFID in such a context. [4 marks]

(*iii*) Most authorities now line the passport sleeve with metal foil. Explain how this increases security and discuss the extent to which it does so. [4 marks]