PD ISO/IEC TS 23220-4:2026

BSI Standards Publication

Cards and security devices for personal identification — Building blocks for identity management via mobile devices

Part 4: Protocols and services for operational phase

National foreword

This Published Document is the UK implementation of ISO/IEC TS 23220-4:2026.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and security devices for personal identification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Attention is drawn to the fact that in the ISO ballot on the final text of this Technical Specification, the UK Committee voted against its approval and recommended that a further draft was necessary. Based on their concerns, the UK committee offers the following information to users.

1. Subclause 6.5.4.3.1: The committee notes that the value for XXXX in the sentence “The 16-bit UUID used shall be the XXXX which is an UUID allocated by the Bluetooth SIG for ISO/IEC JTC SC17” is undefined and recommends that users consult the latest version of the Bluetooth SIG Assigned Numbers document for further guidance on specific UUIDs, or alternatively contact ISO/IEC JTC1 SC17.

2. Subclause 6.5.4.3.2: For more information on the value of the maximum command data length field and the value of the maximum response data length field, in the standard, users are pointed to Subclause 7.4.2.1. The UK committee also points users to Subclause 7.4.1 for more information.

3. Subclause 7.4.2: In the event of a BLE connection drop, although the BLE does have an in-built mechanism for connection/session resumption (as does NFC) the UK Committee suggests users initiate a completely new mdoc transaction (including device engagement) as per the standard’s information on NFC connections in Subclause 7.4.1.

4. Subclauses 6.5.2.1, 6.5.4.1 and 7.3.1 contain statements regarding the protocol flows for Reader Engagement and negotiated handover around handling the possible absence of a Reader Engagement structure. To avoid any potential confusion when applying the different statements, the UK committee suggests that users carefully review how their protocol flows interact with defined engagement structures (see Table 1, Subclause 6.5.2.1).

5. In Subclauses 6.5.4 and 7.4.1 when dealing with NFC transport protocol where there is a connection loss and the user taps the device again quickly, the UK committee suggests users either invalidate the SessionTranscript or establish a grace period before a new DeviceEngagement should be processed.

6. Subclause 6.5.2.2.7 with regard to MAC authentication and static keys explains that mdoc authentication using a MAC (Subclause A.1.3.5) requires the ephemeral reader key to use the same curve as the static device key. However, if a profile mandates specific curves (as noted in Subclause 7.2.1.3.3), but the security mechanisms in Annex A do not provide a fallback for when the reader does not support the mdoc's static key curve, the committee suggest the protocol include a defined error message so the user can distinguish between a legitimate security failure and a simple hardware incompatibility.

7. Subclause 6.6.5 states that the contents of the Handover element used for the SessionTranscript (A.1.6) are "out of scope" for some