

cessing (step 2002). The RFID reader 104 provides an interrogation signal to the RF module 20 for activating the RF module 20 for transaction processing (step 2004). The RF module 20 receives the interrogation signal (step 2006) and the RF module 20 and the RFID reader 104 engage in mutual authentication to determine if each is a valid device for operation on system 100 (step 2008).

[0128] FIG. 22 is a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process is depicted as one-sided. That is, the flowchart depicts the process of the RFID reader 104 authenticating the RF module 20, although similar steps may be followed in the instance that RF module 20 authenticates RFID reader 104. In some embodiments, the RF module 20 and the RFID reader 104 may engage in mutual authentication. In this context, "mutual authentication" may mean that operation of the system 100 may not take place until RF module authenticates the signal from RFID reader 104, and RFID reader 104 authenticates the signal from RF module 20.

[0129] As noted, database 2112 may store security keys for encrypting or decrypting signals received from RF module 20. In an exemplary authentication process, where RFID reader 104 is authenticating RF module 20, RFID reader 104 may provide an interrogation signal to RF module 20 (see step 2002 of FIG. 20). The interrogation signal may include a random code generated by the RFID reader authentication circuit 2110, which is provided to the RF module 20, and which is encrypted using a unique encryption key corresponding to, for example, a RF module 20 unique identification code. In a typical scenario, the protocol/sequence controller 2108 may provide a command to activate the authentication circuitry 2110. Authentication circuitry 2110 may provide from database 2112 an interrogation signal including a random number as a part of the authentication code generated for each authentication signal. The authentication code may be an alphanumeric code which is recognizable (e.g., readable) by the RFID reader 104 and the RF module 20. The authentication code may be provided to the RF module 20 via antenna 2104 (step 2202).

[0130] RF module 20 receives the authentication code (step 2204). The interrogation signal including the authorization code may be received at the RF module antenna 204. The authorization code may be provided to the modulator/demodulator circuit 206 where the signal may be demodulated prior to providing the signal to protocol/sequence controller 208. Protocol/sequence controller 208 may recognize the interrogation signal as a request for authentication of the RF module 20 (step 2206), and provide the authentication code to authentication circuit 210. Authentication circuit 210 or protocol/sequence controller 208 may retrieve an encryption key from database 212 and authentication circuit 210 may encrypt the authentication code using the retrieved encryption key (step 2208). RF module 20 may then provide the encrypted authentication code to the RFID reader 104 for verification (step 2210). The encrypted authentication code may be provided to the RFID reader 104 via RF module modulator/demodulator circuit 206, transponder 214, and antenna 202.

[0131] RFID reader 104 may then receive the encrypted authentication code and decryption it (step 2212). That is, the encrypted authentication code may be received at

antenna 2104 and transponder 2114, and provided to authentication circuit 2110. Authentication circuit 2110 may be provided a security authentication key (e.g., transponder system decryption key) from database 2112. The authentication circuit 2110 may use the authentication key to decrypt (e.g., unlock) the encrypted authorization code. The authentication key may be provided to the authentication circuit 2110 based on the RF module 20 unique identification code. For example, the encrypted authentication code may be provided along with the unique RF module 20 identification code. The authentication circuit 2110 may receive the RF module 20 unique identification code and retrieve from the database 2112 a transponder system decryption key correlative to the unique RF module 20 identification code for use in decrypting the encrypted authentication code.

[0132] Once the authentication code is decrypted (step 2212), the decrypted authentication code is compared to the authentication code provided by the RFID reader 104 to verify its authenticity (step 2214). If the decrypted authorization code is not readable (e.g., recognizable) by the authentication circuit 2110, the RF module 20 is deemed to be unauthorized (e.g., unverified) (step 2216) and the operation of system 100 is terminated (step 2218). Contrarily, if the decrypted authorization code is recognizable (e.g., verified) by the RF module 20, the decrypted authorization code is deemed to be verified or authenticated (step 2220), if so, the transaction is allowed to proceed (step 2222). In one particular embodiment, the proceeding transaction may mean that the RF module 20 may authenticate the RFID reader 104, although, it should be apparent that the RFID reader 104 may authenticate the RF module 20 prior to the RF module 20 authenticating the RFID reader 104.

[0133] With return reference now to FIG. 20, upon successful mutual authentication, the RF module 20 transfers to the RFID reader 104 such data as is necessary to process a transaction request ("user account data") (step 2210).

[0134] The RFID reader 104 receives the user account data at the antenna 2104, and provides the data to the POS interface 2120 (step 2012). In one exemplary embodiment, the RFID reader authentication circuit 2110 may receive the data and provide the data to the RFID reader interface 2120. The RFID reader interface 2120 may then receive the data and convert the data to a merchant POS 110 recognizable format for providing to the merchant system 130. In an exemplary embodiment, the user account data is provided to the RFID reader 104 in magnetic stripe format. In yet another embodiment, the RFID reader 104 provides the user account data to the merchant POS 110 in magnetic stripe format.

[0135] The merchant system 130 may receive the user account data and use the data to form a transaction request (step 2014). The transaction request may include the user account data and any information related to the transaction. The merchant system 130 may provide the transaction request to a user account issuer for processing under business as usual standards (step 2016). Notably, the transaction applications for processing the authentication signal and providing the user account data may be stored in a transaction application on for example, in the database 212 for use by the authentication circuit 210.

[0136] In one exemplary embodiment of the invention, the transaction device 102 (e.g., mobile phone 300) may include