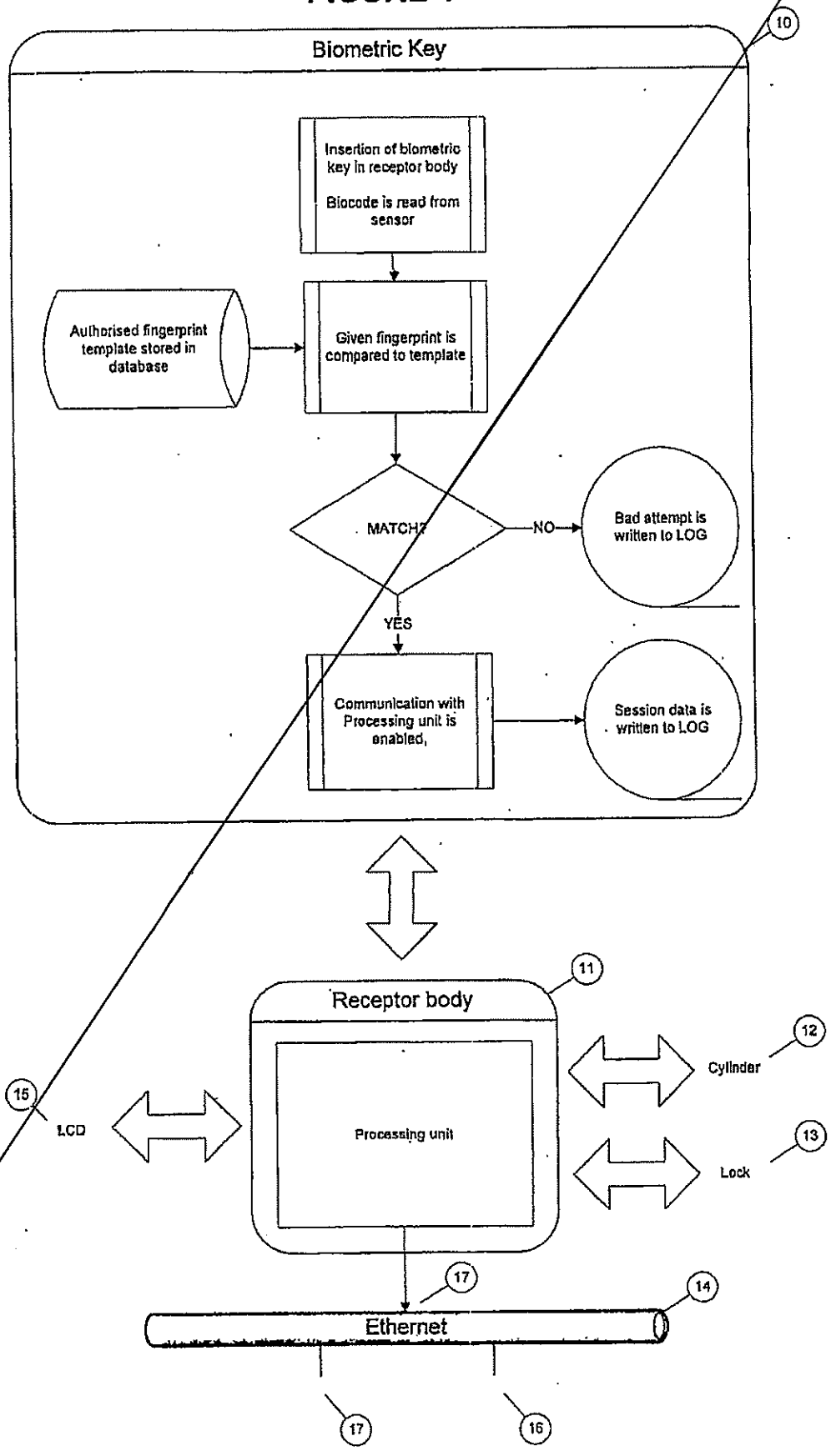
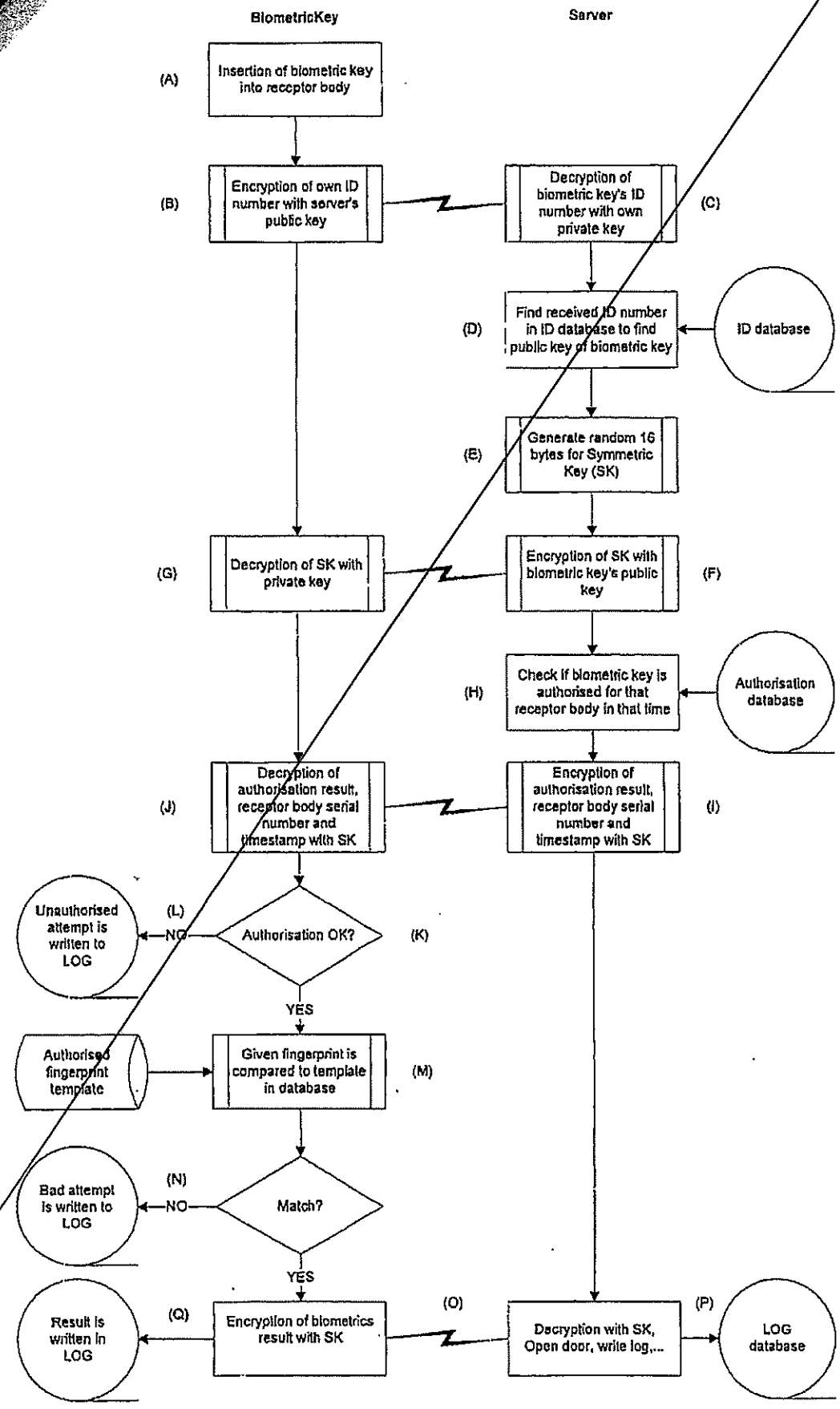
2010224455 28 Sep 2010

FIGURE 1



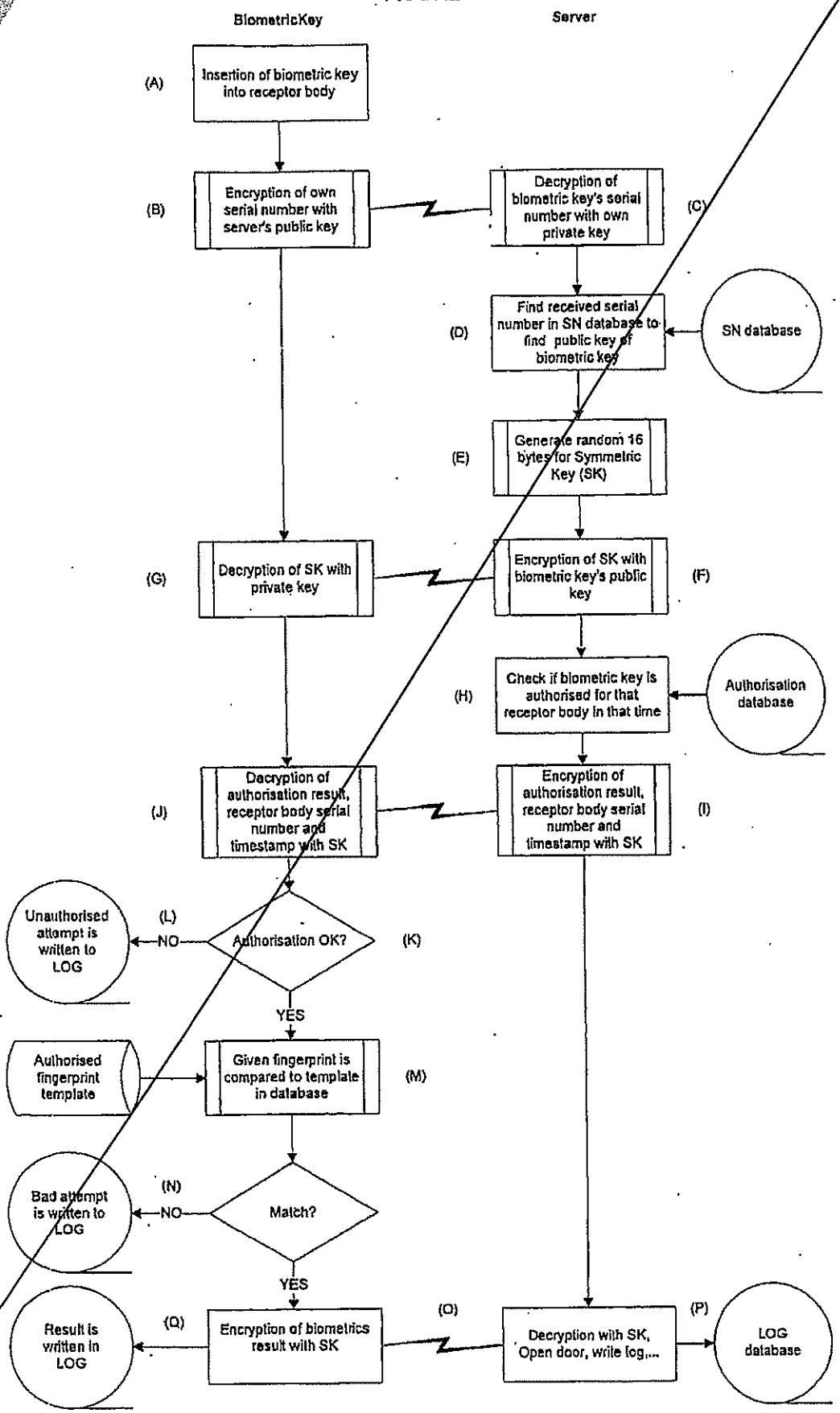
2010224455 28 Sep 2010

FIGURE 2



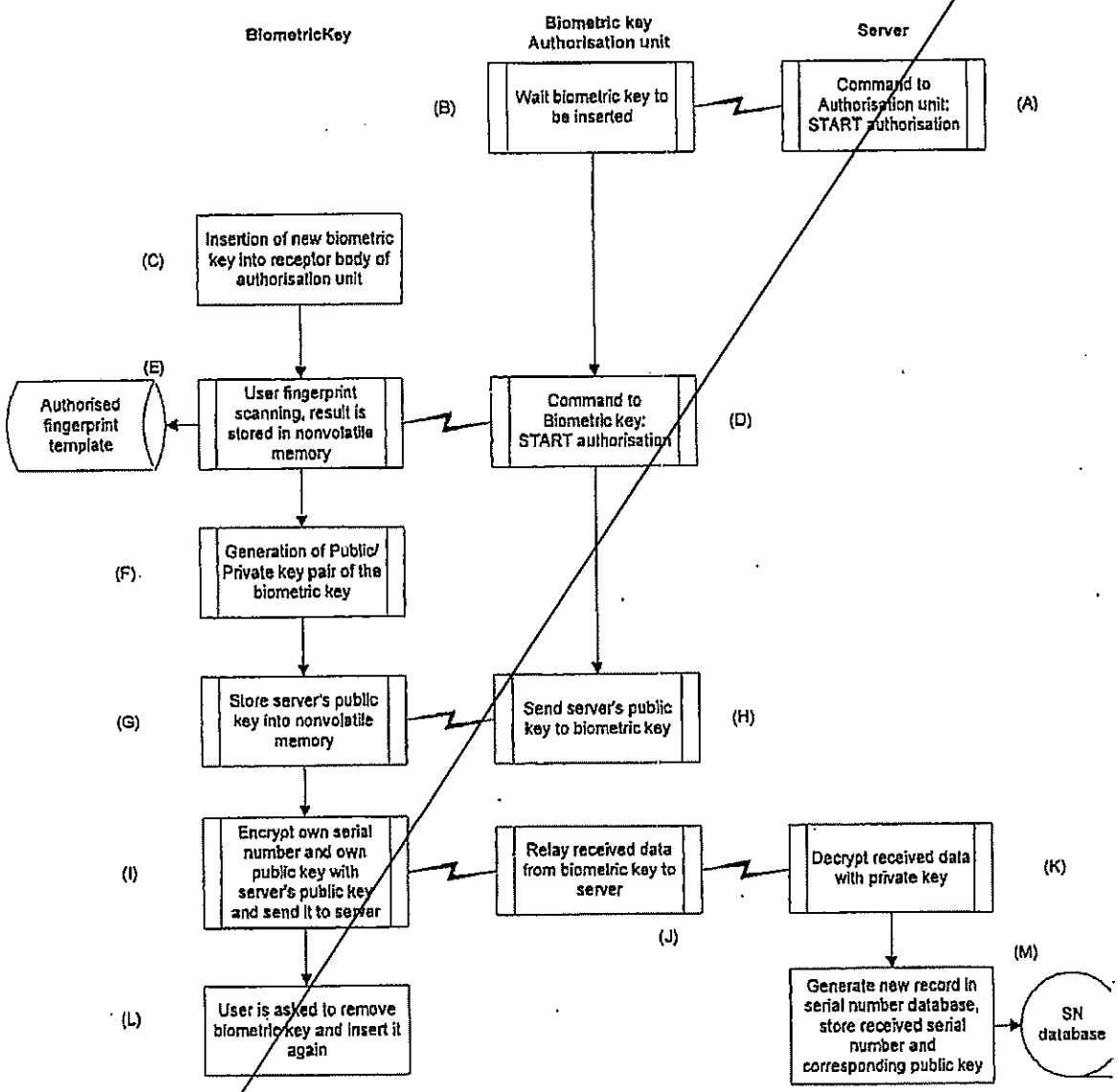
2010224455 28 Sep 2010

FIGURE 3



2010224455 28 Sep 2010

FIGURE 4



28 Sep 2010
2010224455

FIGURE 5

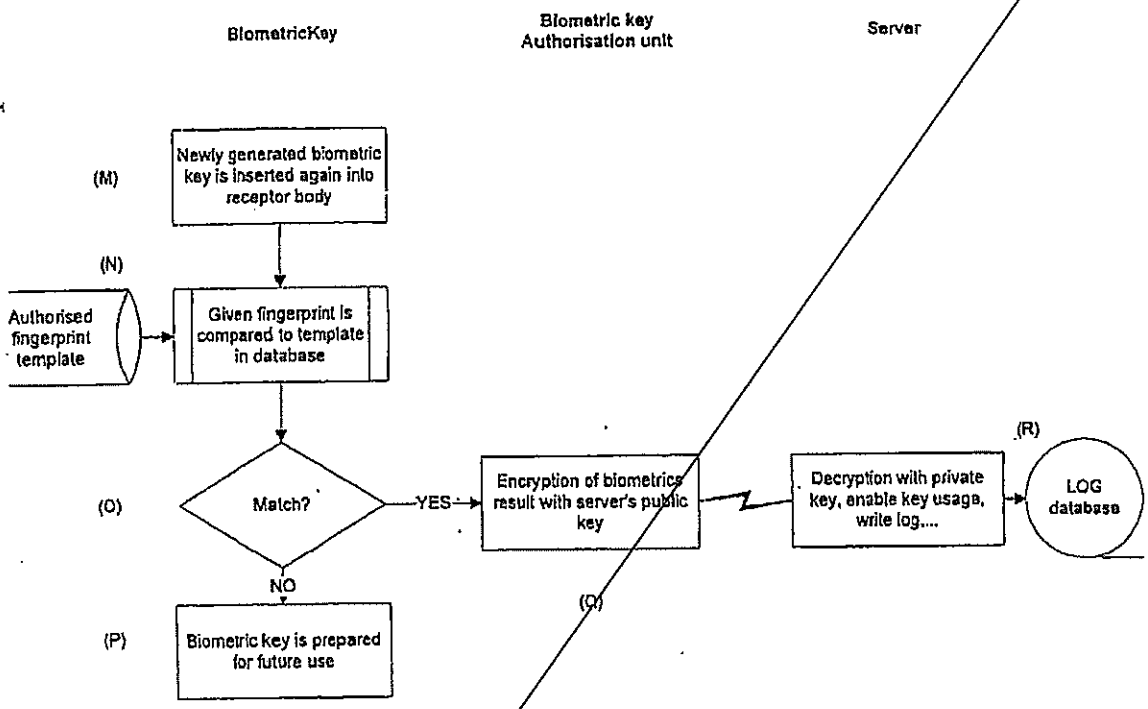


FIGURE 1

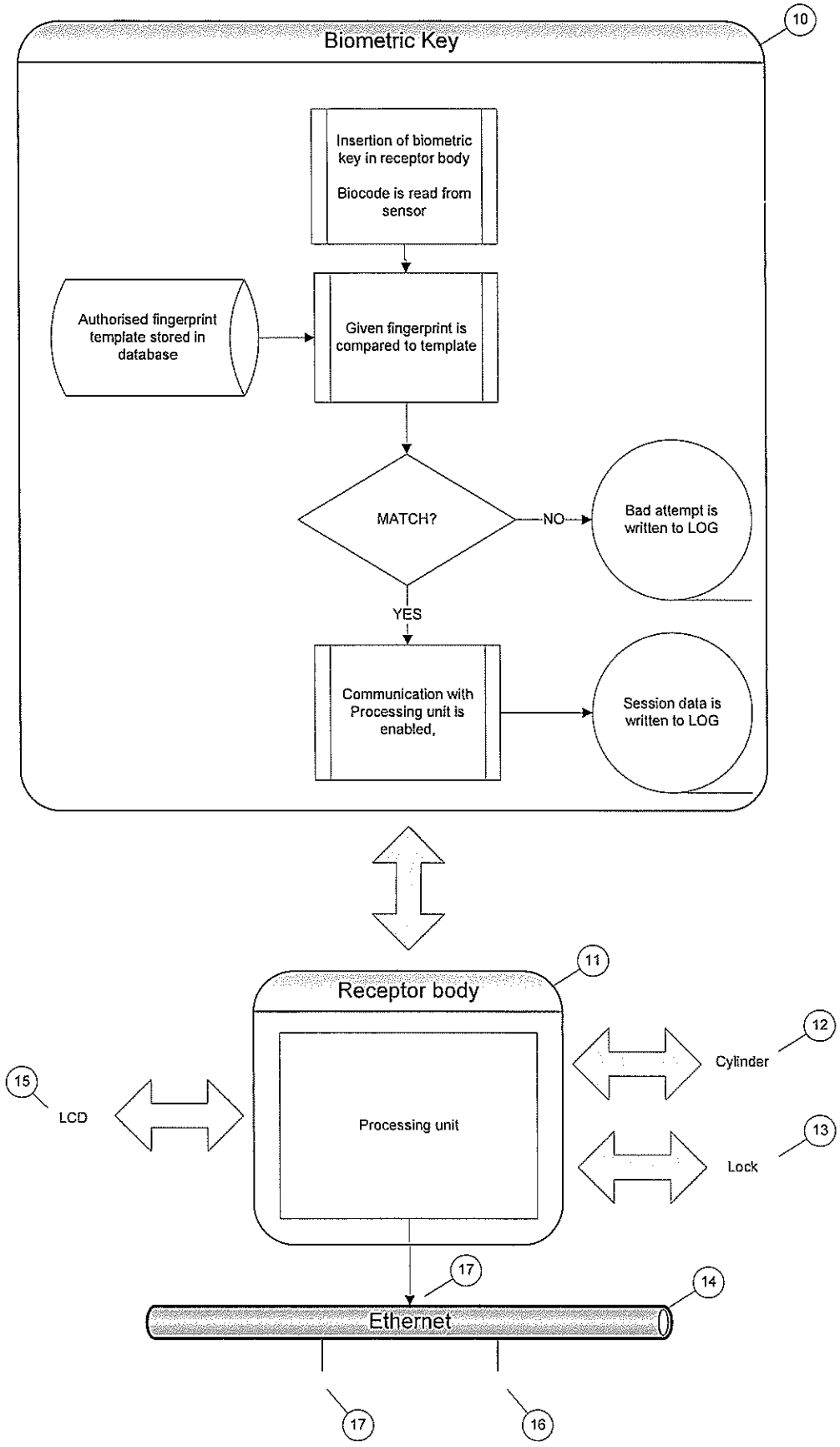

Biometric Key
10
Insertion of biometric key in receptor body
Biocode is read from sensor
Authorised fingerprint template stored in database
Given fingerprint is compared to template
MATCH?
NO
Bad attempt is written to LOG
YES
Communication with Processing unit is enabled,
Session data is written to LOG
11
Receptor body
Processing unit
12
Cylinder
13
Lock
15
LCD
17
14
Ethernet
17
16

FIGURE 2

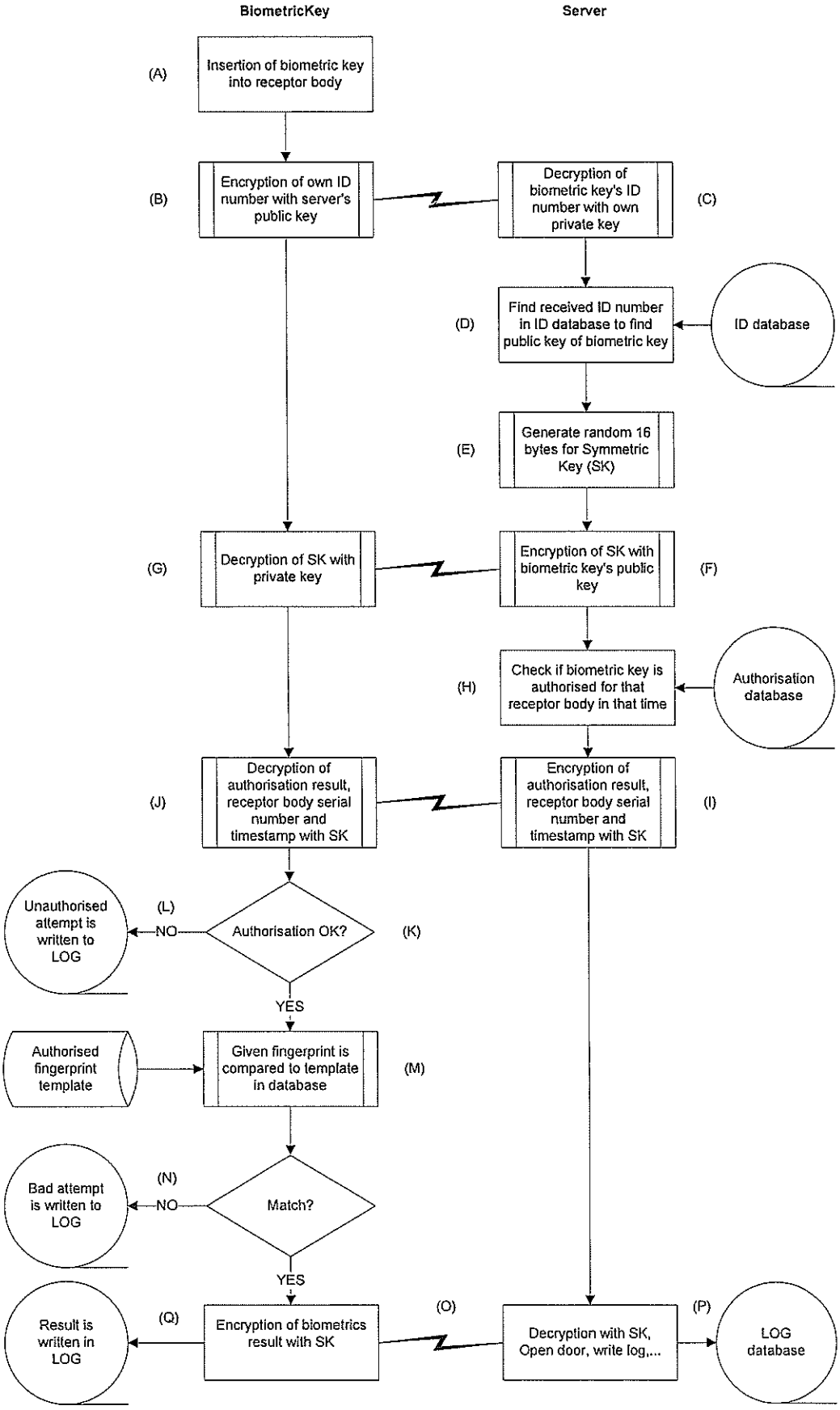

BiometricKey
Server
(A)
Insertion of biometric key into receptor body
(B)
Encryption of own ID number with server's public key
Decryption of biometric key's ID number with own private key
(C)
(D)
Find received ID number in ID database to find public key of biometric key
ID database
(E)
Generate random 16 bytes for Symmetric Key (SK)
(G)
Decryption of SK with private key
Encryption of SK with biometric key's public key
(F)
(H)
Check if biometric key is authorised for that receptor body in that time
Authorisation database
(J)
Decryption of authorisation result, receptor body serial number and timestamp with SK
Encryption of authorisation result, receptor body serial number and timestamp with SK
(I)
Unauthorised attempt is written to LOG
(L)
NO
Authorisation OK?
(K)
YES
Authorised fingerprint template
Given fingerprint is compared to template in database
(M)
Bad attempt is written to LOG
(N)
NO
Match?
YES
Result is written in LOG
(Q)
Encryption of biometrics result with SK
(O)
Decryption with SK, Open door, write log,...
(P)
LOG database

FIGURE 3

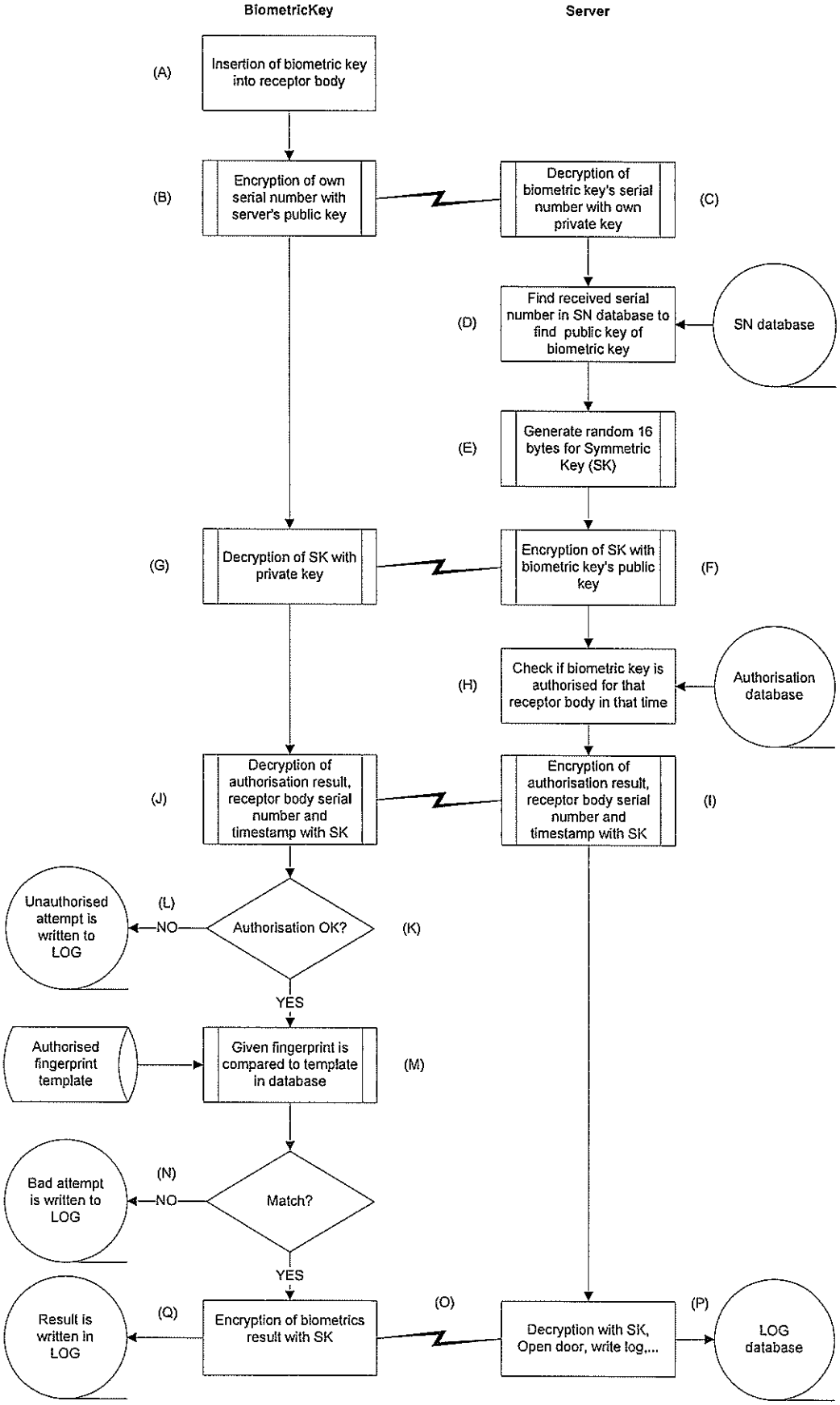

BiometricKey
Server
(A)
Insertion of biometric key into receptor body
(B)
Encryption of own serial number with server's public key
Decryption of biometric key's serial number with own private key
(C)
(D)
Find received serial number in SN database to find public key of biometric key
SN database
(E)
Generate random 16 bytes for Symmetric Key (SK)
(G)
Decryption of SK with private key
Encryption of SK with biometric key's public key
(F)
(H)
Check if biometric key is authorised for that receptor body in that time
Authorisation database
(J)
Decryption of authorisation result, receptor body serial number and timestamp with SK
Encryption of authorisation result, receptor body serial number and timestamp with SK
(I)
Unauthorised attempt is written to LOG
(L)
NO
Authorisation OK?
(K)
YES
Authorised fingerprint template
Given fingerprint is compared to template in database
(M)
Bad attempt is written to LOG
(N)
NO
Match?
YES
Result is written in LOG
(Q)
Encryption of biometrics result with SK
(O)
Decryption with SK, Open door, write log,...
(P)
LOG database

FIGURE 4

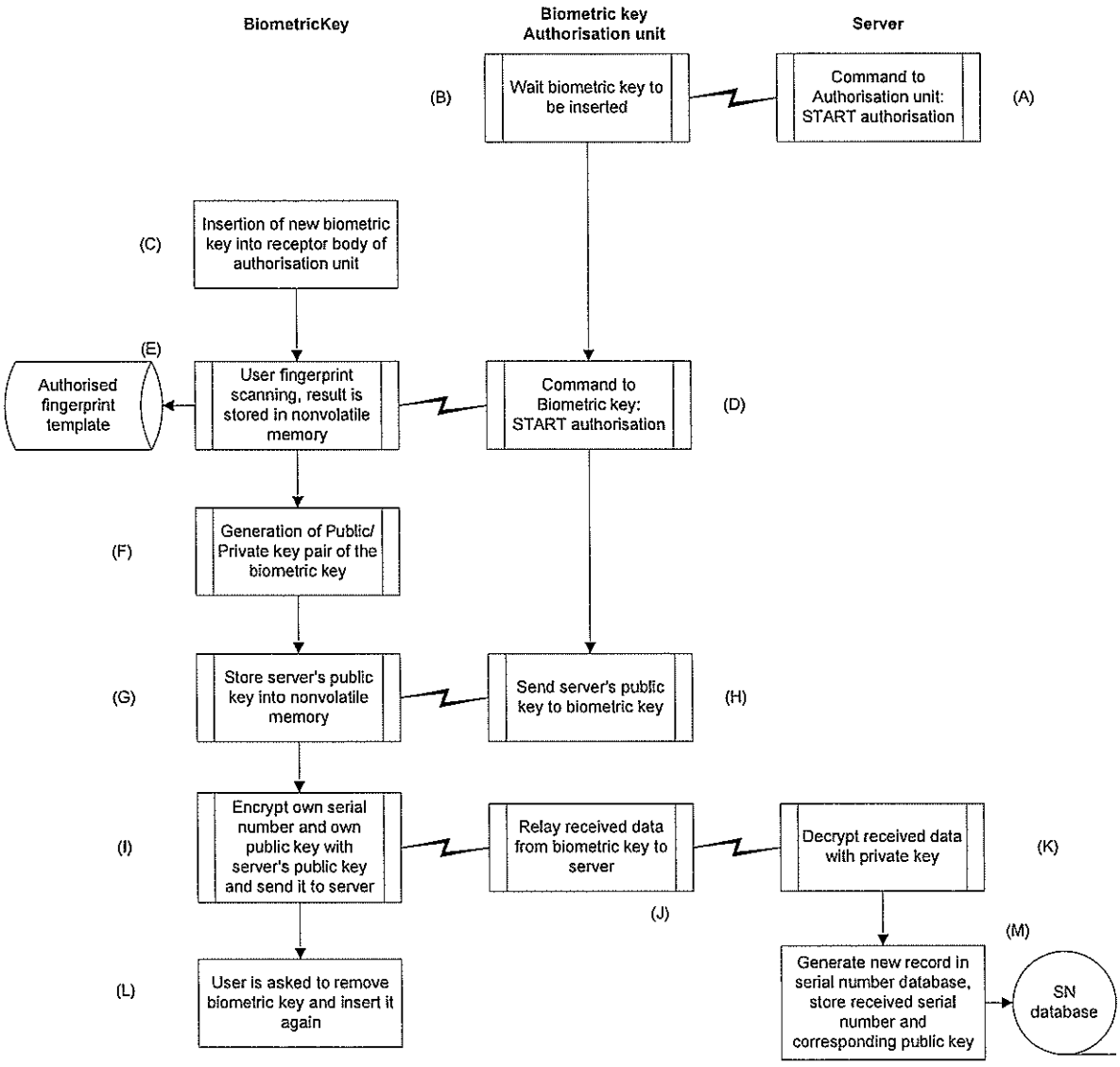
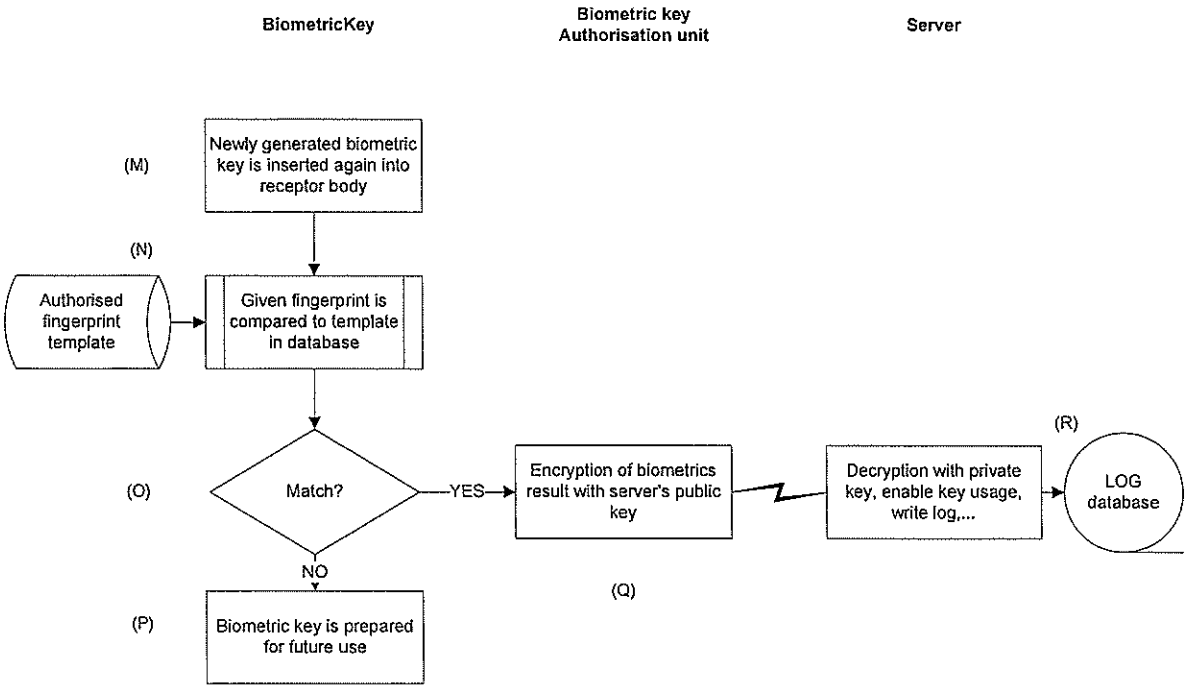

BiometricKey
Biometric key Authorisation unit
Server
(A)
Command to Authorisation unit: START authorisation
(B)
Wait biometric key to be inserted
(C)
Insertion of new biometric key into receptor body of authorisation unit
(D)
Command to Biometric key: START authorisation
(E)
User fingerprint scanning, result is stored in nonvolatile memory
Authorised fingerprint template
(F)
Generation of Public/ Private key pair of the biometric key
(G)
Store server's public key into nonvolatile memory
(H)
Send server's public key to biometric key
(I)
Encrypt own serial number and own public key with server's public key and send it to server
(J)
Relay received data from biometric key to server
(K)
Decrypt received data with private key
(L)
User is asked to remove biometric key and insert it again
(M)
Generate new record in serial number database, store received serial number and corresponding public key
SN database

FIGURE 5


BiometricKey
Biometric key Authorisation unit
Server
(M)
Newly generated biometric key is inserted again into receptor body
(N)
Authorised fingerprint template
Given fingerprint is compared to template in database
(O)
Match?
YES
NO
Encryption of biometrics result with server's public key
(Q)
Decryption with private key, enable key usage, write log,...
(R)
LOG database
(P)
Biometric key is prepared for future use