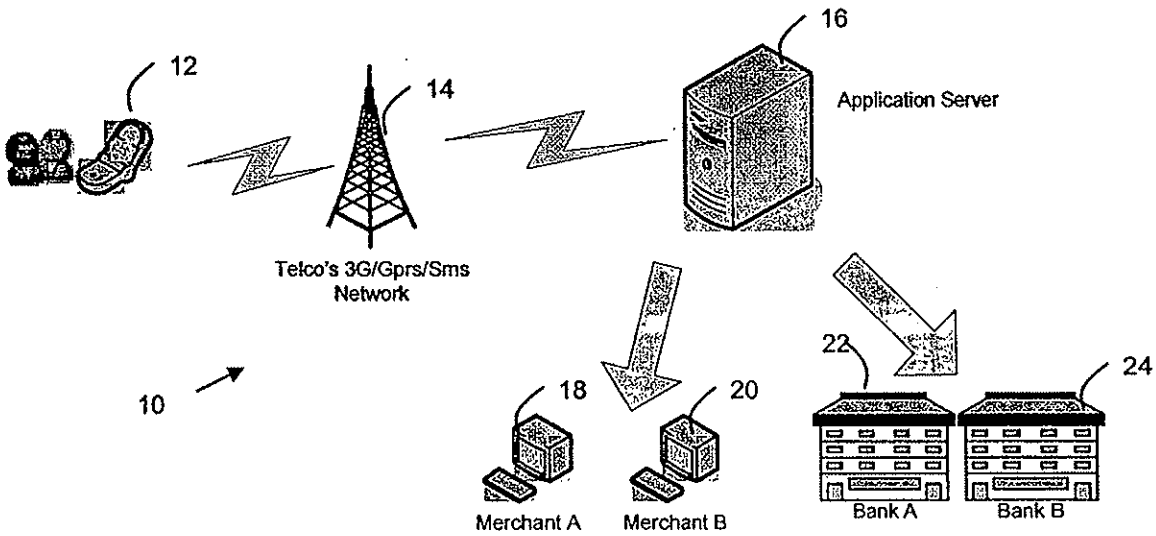

12
14
16
Application Server
Telco's 3G/Gprs/Sms Network
10
18
20
22
24
Merchant A
Merchant B
Bank A
Bank B

FIG. 1

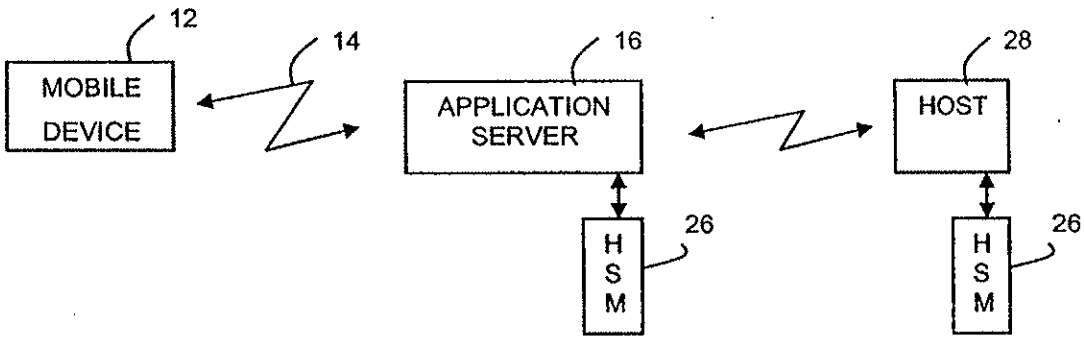

12
MOBILE DEVICE
14
16
APPLICATION SERVER
28
HOST
26
H S M
26
H S M

FIG. 2

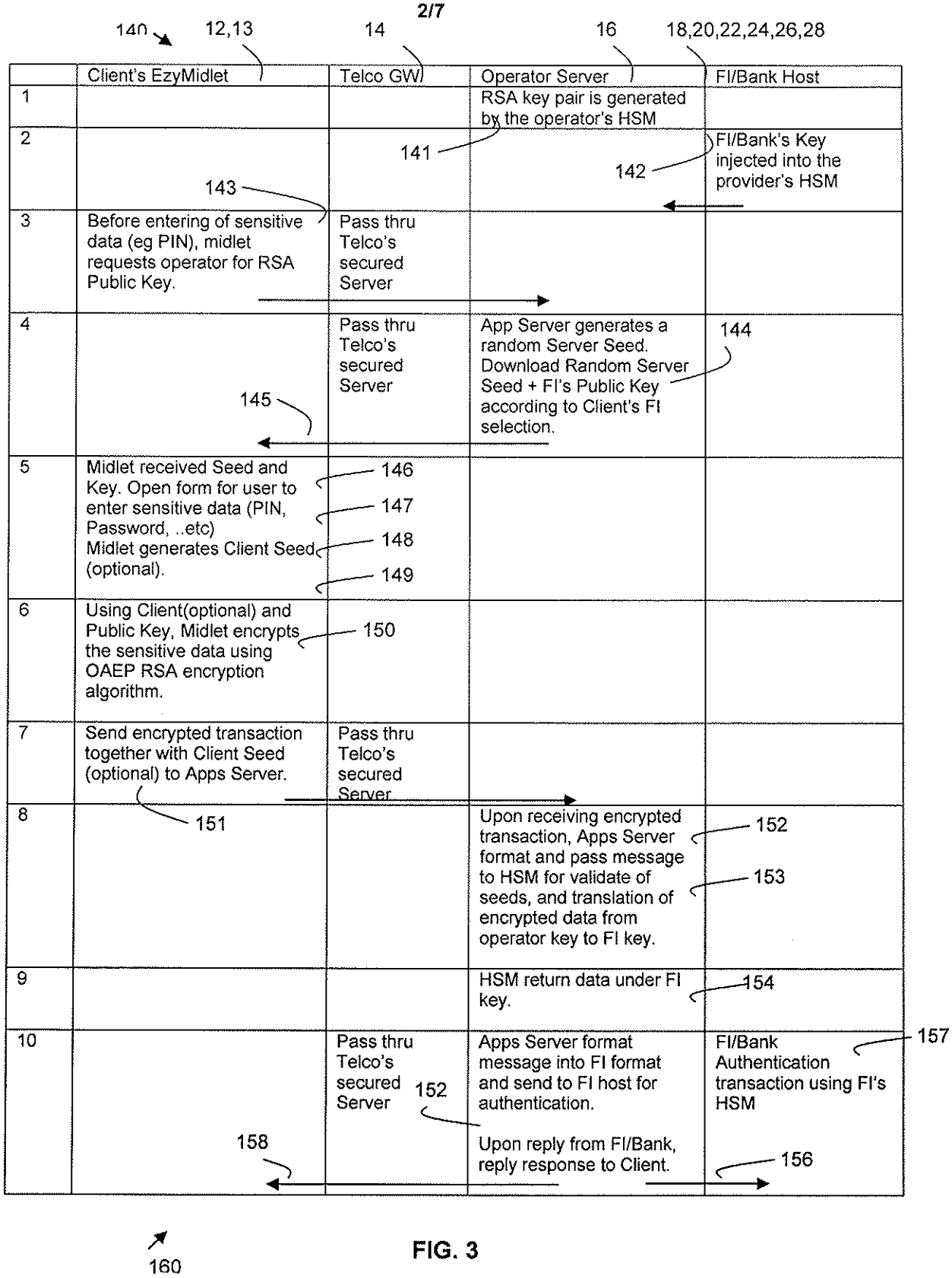

140
12,13
14
16
18,20,22,24,26,28
Client's EzyMidlet
Telco GW
Operator Server
FI/Bank Host
1
RSA key pair is generated by the operator's HSM
2
141
142
FI/Bank's Key injected into the provider's HSM
143
3
Before entering of sensitive data (eg PIN), midlet requests operator for RSA Public Key.
Pass thru Telco's secured Server
4
Pass thru Telco's secured Server
App Server generates a random Server Seed. Download Random Server Seed + FI's Public Key according to Client's FI selection.
144
145
5
Midlet received Seed and Key. Open form for user to enter sensitive data (PIN, Password, ..etc)
Midlet generates Client Seed (optional).
146
147
148
149
6
Using Client(optional) and Public Key, Midlet encrypts the sensitive data using OAEP RSA encryption algorithm.
150
7
Send encrypted transaction together with Client Seed (optional) to Apps Server.
Pass thru Telco's secured Server
8
151
Upon receiving encrypted transaction, Apps Server format and pass message to HSM for validate of seeds, and translation of encrypted data from operator key to FI key.
152
153
9
HSM return data under FI key.
154
10
Pass thru Telco's secured Server
152
Apps Server format message into FI format and send to FI host for authentication.
Upon reply from FI/Bank, reply response to Client.
FI/Bank Authentication transaction using FI's HSM
157
156
158
160

FIG. 3

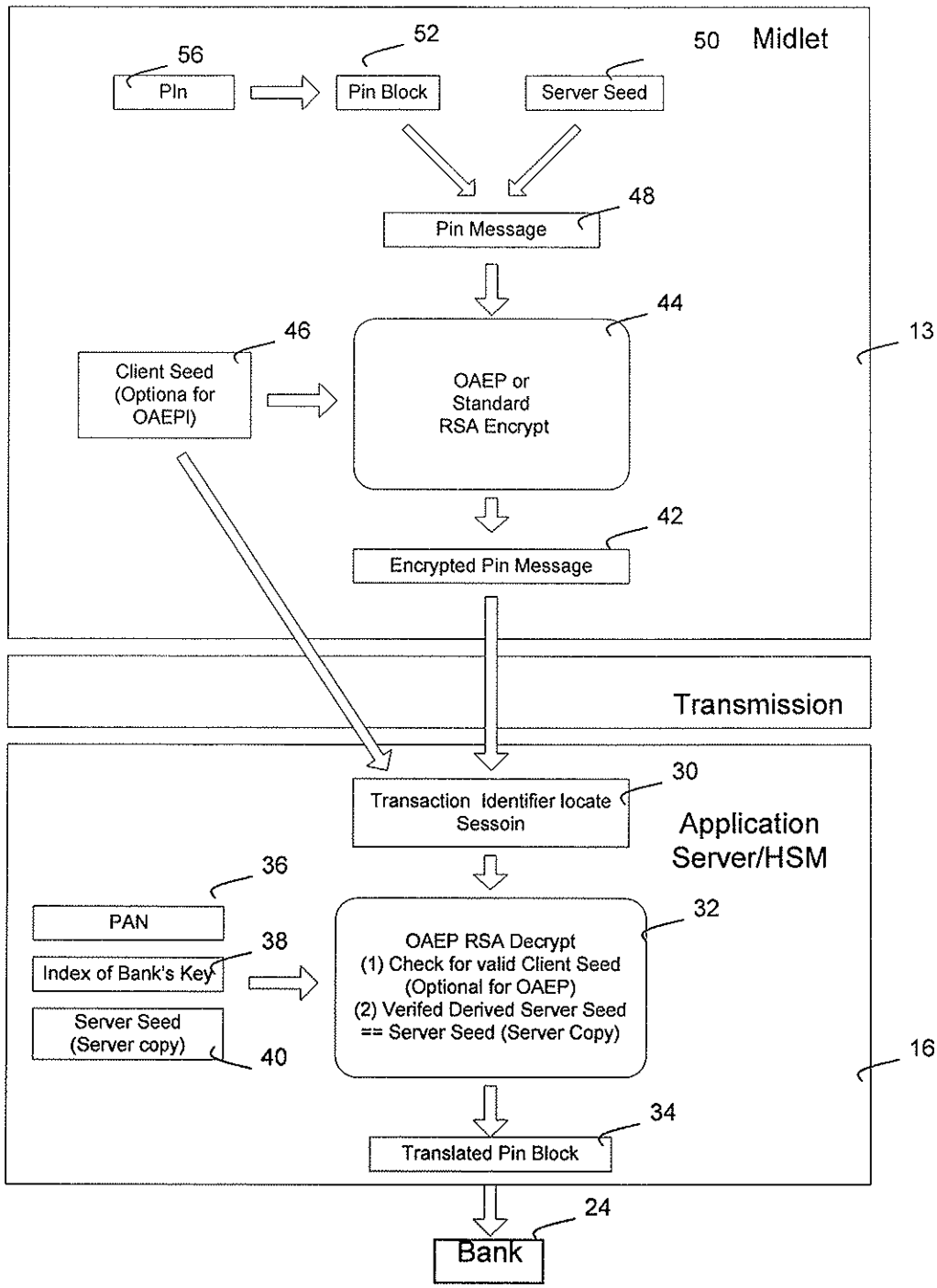

56
Pin
52
Pin Block
Server Seed
50
Midlet
48
Pin Message
44
46
Client Seed
(Optiona for
OAEPl)
OAEP or
Standard
RSA Encrypt
13
42
Encrypted Pin Message
Transmission
30
Transaction Identifier locate
Sessoin
Application
Server/HSM
36
PAN
38
Index of Bank's Key
Server Seed
(Server copy)
40
OAEP RSA Decrypt
(1) Check for valid Client Seed
(Optional for OAEP)
(2) Verifed Derived Server Seed
== Server Seed (Server Copy)
32
16
34
Translated Pin Block
24
Bank

FIG.4

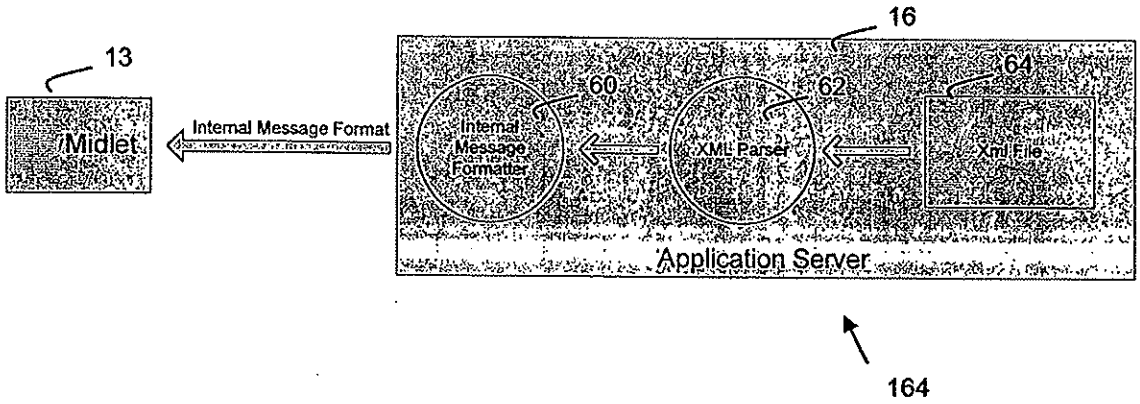



FIG. 5

| Msg ID | Message Format | Remarks |
|---|---|---|
| 90 | 90\|next file id>\|<cur file id> | Get next screen |
| | Eg. 90\|002\|001 | |
| 95 | 95\|<mer_id>\|<amount>\|<mps > | Get txn details |
| | Eg. 95\|001\|19.80\|223344 | |
| 96 | 96\| | Get last 5 txn request |
| | Eg. 96\| | |
| 97 | 97\| | Get bank list |
| | Eg. 97\| | |
| 98 | 98\|<midlet version>\|<file id>;<footprint>\|..... | Initial login and record store cache info. If record store is empty, only the <midlet version> will be sent. |
| | Eg. 98\|3.5\|1;157894\|2;465879\|.... | |
| 99 | 99\|<return param>\|..... | Form submit |
| | Eg. 99\|account=1233\|amount=25.74\|mer_id=M1\|bank_acct_type=SavingAccount\|bank_u_id=ezypay\|bank_u_pin=I0AyKhswoxjmehrz9fGp4s0X+ | |

FIG. 7

180

| Tags | Description | Remarks | Attributes | Attributes Remarks |
|---|---|---|---|---|
| *<owner>* | Page owner | • mer_id in table mer_profile | | |
| *<next_file>* | Next file id | • file_id in table xml_table | | |
| *<page_type>* | Page attribute | List | | |
| | | Form | | |
| *<title>* | Page title | | | |
| *<list>* | List item | | image | Image file name |
| | | | file | Next file name |
| *<choice>* | Choice item | • Display choice heading and items | value | Choice items separated by "," |
| | | | param | Field param to be returned to servlet |
| *<input_field>* | Input item | • If no default value, must contain a " " or a missing </input_field > | label | String label |
| | | | att | 01 – text decimal<br>02 – text number<br>03 – text password<br>04 – text alphanumeric<br>05 – text numeric |
| | | | size | Length of input |
| | | | param | Field param to be returned to servlet |
| *<image>* | Image item | • Display text followed by image | img | Image file name |
| *<text_field>* | Display string | • Display text string | text | Display bold text string |
| *<spacer>* | Spacer item | | | |
| *<ticker>* *(Not in use)* | Ticker item | • If value = "random-<mer_id>" ➔ ticker message will be picked randomly from table ad_ticker. | | |

**FIG. 6**

170

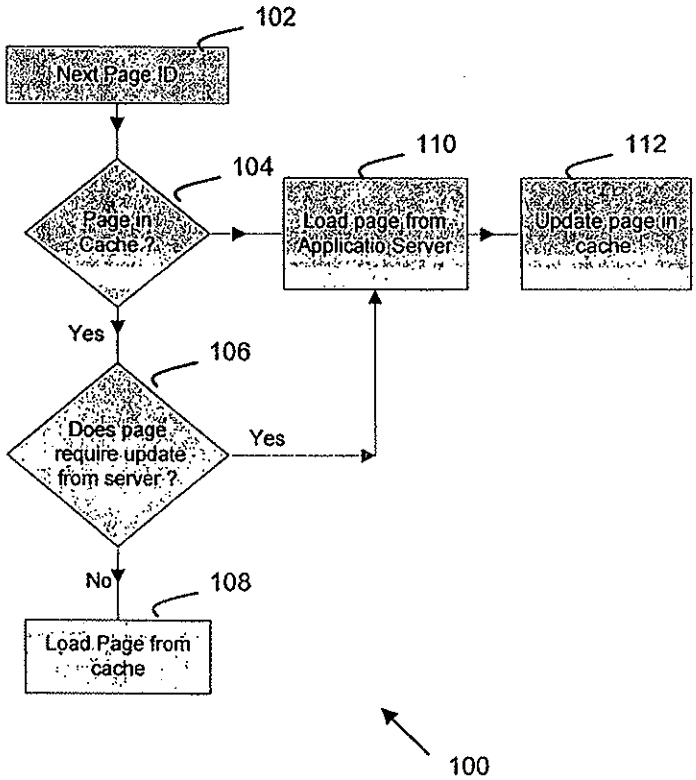

102
Next Page ID
104
Page in Cache ?
110
Load page from Application Server
112
Update page in cache
Yes
106
Does page require update from server ?
Yes
No
108
Load Page from cache
100

FIG. 8

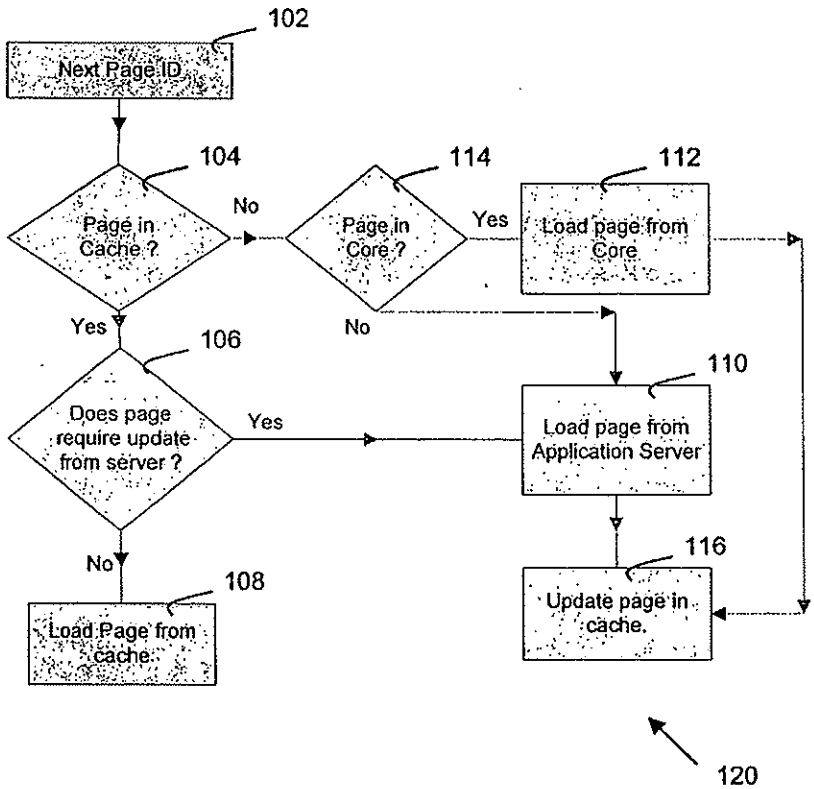

102
Next Page ID
104
Page in Cache ?
No
114
Page in Core ?
Yes
112
Load page from Core
Yes
No
106
Does page require update from server ?
Yes
110
Load page from Application Server
No
108
Load Page from cache
116
Update page in cache.
120

FIG. 9