

Claims

1. A method for securing a transaction by a user comprising:
providing a subscriber unit having a processor, a memory, and a display,
wherein said subscriber unit is configured to accept user input,
providing a credential information manager having a processor and a memory,
storing a cyber identifier associated with the user in said credential information
manager memory;
storing a subscriber identifier associated with the user in said credential information
manager memory;
storing subscriber information associated with the user in said credential information
manager memory;
providing a transaction service provider having a processor and a memory,
transmitting a request for a transaction from said subscriber unit to said transaction
service provider;
transmitting a transaction identifier, created by said transaction service provider based
on said transaction request, from said transaction service provider to said
subscriber unit;
storing said transaction identifier in said transaction service provider memory;
transmitting a request for authentication from said subscriber unit to said credential
information manager;
transmitting said transaction identifier from said subscriber unit to said credential
information manager;
transmitting a subscriber identifier from said subscriber unit to said credential
information manager;

authenticating, by said credential information manager, said subscriber identifier received by said credential information manager from said subscriber unit with said subscriber identifier stored in said credential information manager memory;

transmitting a request for verification from said credential information manager to said transaction service provider

transmitting, from said credential information manager to said transaction service provider, said transaction identifier received from said subscriber unit;

verifying, by transaction service provider, said transaction identifier received by transaction service provider from said credential information manager with said transaction identifier stored in said transaction service provider memory;

transmitting, from said transaction service provider to said credential information manager, a verification request result message;

transmitting, from said credential information manager to said transaction service provider, said cyber identifier stored in said credential information manager memory;

transmitting, from said credential information manager to said transaction service provider, said subscriber information stored in said credential information manager memory; and

transmitting a transaction authorization from said credential information manager to said transaction service provider.

2. The method of claim 1 wherein said authentication further includes comparing, by said credential information manager processor, said subscriber identifier received by said credential information manager from said subscriber unit with said subscriber identifier stored in said credential information manager memory.

3. The method of claim 2 wherein said verification request is sent as a result of said comparison indicating that said subscriber identifier received by said credential information manager from said subscriber unit matches said subscriber identifier stored in said credential information manager memory.
4. The method of claim 2 further including transmitting an authentication failure message from said credential information manager to said subscriber unit, wherein said authentication failure message is sent as a result of said comparison indicating that said subscriber identifier received by said credential information manager from said subscriber unit does not match said subscriber identifier stored in said credential information manager memory.
5. The method of claim 4 further including displaying a visual authentication failure message on said subscriber unit display based on said authentication failure message transmitted from said credential information manager to said subscriber unit.
6. The method of claim 1 wherein said verification further includes comparing, by said transaction service provider processor, said transaction identifier received by transaction service provider from said credential information manager with said transaction identifier stored in said transaction service provider memory, wherein said verification result request message includes a result of said comparison.
7. The method of claim 6 wherein said transmission of said cyber identifier is sent as a result of said verification result request message indicating that said transaction identifier received by said transaction service provider from said credential information manager matches with said transaction identifier stored in said transaction service provider memory.
8. The method of claim 6 further including transmitting a verification failure message from said credential information manager to said subscriber unit, wherein said verification

failure message is sent as a result of said verification result request message indicating that said transaction identifier received by said transaction service provider from said credential information manager does not match with said transaction identifier stored in said transaction service provider memory.

9. The method of claim 8 further including displaying a visual verification failure message on said subscriber unit display based on said verification failure message transmitted from said credential information manager to said subscriber unit.
10. The method of claim 1 wherein said subscriber unit is made up of one or more mobile phones, smart phones, PDAs, computers, or POS terminals, modems, fax machines, or display/input terminals.
11. The method of claim 10 wherein said subscriber unit is made of a phone in wireless communication with a POS terminal.
12. The method of claim 1 where one or more of the transmissions are made via a secure telecommunications link.
13. The method of claim 1 where one or more of the transmissions are made via a wireless telecommunications link.
14. The method of claim 1 where one or more of the transmissions are made via the internet.
15. The method of claim 12 wherein said secure telecommunications link includes one or more of a VPN, audio or visual signalling, secure tunnelling, or an encrypted communication infrastructure.
16. The method of claim 1 wherein, before said subscriber identifier is transmitted from said subscriber unit to said credential information manager, said subscriber identifier is received as input to the subscriber unit and stored in said subscriber unit memory.
17. The method of claim 1 wherein said subscriber unit memory includes a removable memory, and before said subscriber identifier is transmitted from said subscriber unit

to said credential information manager, said subscriber identifier is stored in said subscriber unit memory.

18. The method of claim 17 wherein said removable memory includes a SIM card.
19. The method of claim 17 wherein said removable memory includes an electronic card.
20. The method of claim 1 further including storing said subscriber information, transmitted from said credential information manager to said transaction service provider, in said transaction service provider memory.
21. The method of claim 1 further including transmitting said subscriber information, transmitted from said credential information manager to said transaction service provider, from said transaction service provider to said subscriber unit.
22. The method of claim 21 further including displaying visual subscriber information on said subscriber unit display based on said subscriber information transmitted from said transaction service provider to said subscriber unit.

23. A method for securing a transaction among a user, a credential information manager, and a transaction service provider comprising:
- providing a subscriber unit having a processor, a memory, and a display,
 - wherein said subscriber unit is configured to accept user input,
 - transmitting a request for a transaction from said subscriber unit to the transaction service provider;
 - receiving, by said subscriber unit, a transaction identifier transmitted from said transaction service provider;
 - transmitting a request for authentication from said subscriber unit to said credential information manager;
 - transmitting said transaction identifier from said subscriber unit to said credential information manager; and
 - transmitting a subscriber identifier from said subscriber unit to said credential information manager.
24. The method of claim 23 further including receiving, by said subscriber unit, an authentication failure message from the credential information manager to said subscriber unit, wherein said authentication failure message indicates that said subscriber identifier transmitted to the credential information manager by said subscriber unit does not match a subscriber identifier stored in a memory of the credential information manager.
25. The method of claim 24 further including displaying a visual authentication failure message on said subscriber unit display based on said authentication failure message received from the credential information manager by said subscriber unit.
26. The method of claim 23 further including receiving, by said subscriber unit, a verification failure message from the credential information manager, wherein said verification

failure message indicates that a transaction identifier received by the transaction service provider from said credential information manager does not match with a transaction identifier stored in said transaction service provider memory.

27. The method of claim 26 further including displaying a visual verification failure message on said subscriber unit display based on said verification failure message transmitted from the credential information manager to said subscriber unit.
28. The method of claim 23 wherein said subscriber unit is made up of one or more mobile phones, smart phones, PDAs, computers, or POS terminals, modems, fax machines, or display/input terminals.
29. The method of claim 28 wherein said subscriber unit is made of a phone in wireless communication with a POS terminal.
30. The method of claim 23 where one or more of the transmissions received or transmitted by said subscriber unit are made via a secure telecommunications link.
31. The method of claim 23 where one or more of the transmissions received or transmitted by said subscriber unit are made via a wireless telecommunications link.
32. The method of claim 23 where one or more of the transmissions received or transmitted by said subscriber unit are made via the internet.
33. The method of claim 30 wherein said secure telecommunications link includes one or more of a VPN, audio or visual signalling, secure tunnelling, or an encrypted communication infrastructure.
34. The method of claim 23 wherein, before said subscriber identifier is transmitted from said subscriber unit to the credential information manager, said subscriber identifier is received as input to the subscriber unit and stored in said subscriber unit memory.
35. The method of claim 23 wherein said subscriber unit memory includes a removable memory, and before said subscriber identifier is transmitted from said subscriber unit

to said credential information manager, said subscriber identifier is stored in said subscriber unit memory.

36. The method of claim 35 wherein said removable memory includes a SIM card.
37. The method of claim 35 wherein said removable memory includes an electronic card.
38. The method of claim 23 further including receiving, by said subscriber unit, subscriber information from the transaction service provider.
39. The method of claim 38 further including displaying visual subscriber information on said subscriber unit display based on said subscriber information transmitted from the transaction service provider to said subscriber unit.

40. A method for securing a transaction among a user, a subscriber unit, and a transaction service provider comprising:

providing a credential information manager having a processor and a memory,

storing a cyber identifier associated with the user in said credential information

manager memory;

storing a subscriber identifier associated with the user in said credential information

manager memory;

storing subscriber information associated with the user in said credential information

manager memory;

receiving, by said credential information manager, a request for authentication from

the subscriber unit;

receiving, by said credential information manager, said transaction identifier from the

subscriber unit;

receiving, by said credential information manager, a subscriber identifier from the

subscriber unit;

authenticating, by said credential information manager, said subscriber identifier

received by said credential information manager from said subscriber unit with

said subscriber identifier stored in said credential information manager

memory;

transmitting a request for verification from said credential information manager to the

transaction service provider;

transmitting, from said credential information manager to the transaction service

provider, said transaction identifier received from the subscriber unit;

receiving, by said credential information manager, a verification request result

message from the transaction service provider;

transmitting, from said credential information manager to said transaction service provider, said cyber identifier stored in said credential information manager memory;

transmitting, from said credential information manager to said transaction service provider, said subscriber information stored in said credential information manager memory; and

transmitting a transaction authorization from said credential information manager to said transaction service provider.

41. The method of claim 40 wherein said authentication further includes comparing, by said credential information manager processor, said subscriber identifier received by said credential information manager from the subscriber unit with said subscriber identifier stored in said credential information manager memory.

42. The method of claim 41 wherein said verification request is sent as a result of said comparison indicating that said subscriber identifier received by said credential information manager from the subscriber unit matches said subscriber identifier stored in said credential information manager memory.

43. The method of claim 42 further including transmitting an authentication failure message from said credential information manager to the subscriber unit, wherein said authentication failure message is sent as a result of said comparison indicating that said subscriber identifier received by said credential information manager from the subscriber unit does not match said subscriber identifier stored in said credential information manager memory.

44. The method of claim 40 wherein said transmission of said cyber identifier is sent as a result of said verification result request message indicating that said transaction identifier transmitted to the transaction service provider by said credential information

manager matches with a transaction identifier stored in the transaction service provider memory.

45. The method of claim 40 further including transmitting a verification failure message from said credential information manager to the subscriber unit, wherein said verification failure message is sent as a result of said verification result request message indicating that said transaction identifier transmitted to said transaction service provider by said credential information manager does not match with said transaction identifier stored in said transaction service provider memory.
46. The method of claim 40 where one or more of the transmissions received or transmitted by said credential information manager are made via a secure telecommunications link.
47. The method of claim 40 where one or more of the transmissions received or transmitted by said credential information manager are made via a wireless telecommunications link.
48. The method of claim 40 where one or more of the transmissions received or transmitted by said credential information manager are made via the internet.
49. The method of claim 46 wherein said secure telecommunications link includes one or more of a VPN, audio or visual signalling, secure tunnelling, or an encrypted communication infrastructure.

50. A method for securing a transaction among a user, a subscriber unit, and a credential information manager comprising:

providing a transaction service provider having a processor and a memory,
transmitting a request for a transaction from the subscriber unit to said transaction service provider;
transmitting a transaction identifier, created by said transaction service provider based on said transaction request, from said transaction service provider to the subscriber unit;
storing said transaction identifier in said transaction service provider memory;
receiving, by the transaction service provider, a request for verification from the credential information manager;
receiving a transaction identifier, by the transaction service provider, from said credential information manager;
verifying, by said transaction service provider, said transaction identifier received by said transaction service provider from the credential information manager with said transaction identifier stored in said transaction service provider memory;
transmitting, from said transaction service provider to the credential information manager, a verification request result message;
receiving, by the transaction service provider from the credential information manager, a cyber identifier;
receiving, by the transaction service provider from the credential information manager, subscriber information associated with the user; and
receiving, by said transaction service provider from the credential information manager, a transaction authorization.

51. The method of claim 50 wherein said verification further includes comparing, by said transaction service provider processor, said transaction identifier received by said transaction service provider from the credential information manager with said transaction identifier stored in said transaction service provider memory, wherein said verification result request message includes a result of said comparison.
52. The method of claim 50 where one or more of the transmissions received or transmitted by said transaction service provider are made via a secure telecommunications link.
53. The method of claim 50 where one or more of the transmissions received or transmitted by said transaction service provider are made via a wireless telecommunications link.
54. The method of claim 50 where one or more of the transmissions received or transmitted by said transaction service provider are made via the internet.
55. The method of claim 52 wherein said secure telecommunications link includes one or more of a VPN, audio or visual signalling, secure tunnelling, or an encrypted communication infrastructure.
56. The method of claim 50 further including storing said subscriber information, received by said transaction service provider from the credential information manager, in said transaction service provider memory.
57. The method of claim 50 further including transmitting said subscriber information, received by said transaction service provider from the credential information manager, from said transaction service provider to the subscriber unit.

58. A system for securing a transaction by a user comprising:
- a subscriber unit having a processor, a memory, and a display,
 - wherein said subscriber unit is configured to accept user input,
 - a credential information manager having a processor and a memory,
 - a cyber identifier associated with the user stored in said credential information manager memory;
 - a subscriber identifier associated with the user stored in said credential information manager memory;
 - subscriber information associated with the user stored in said credential information manager memory;
 - a transaction service provider having a processor and a memory,
 - a communication path for transmitting a request for a transaction from said subscriber unit to said transaction service provider;
 - a computer program stored in said memory of said transaction service provider for
 - creating, based on said transaction request, a transaction identifier;
 - a communication path for transmitting said transaction identifier created by said transaction service provider to said subscriber unit;
 - a transaction identifier stored in said transaction service provider memory;
 - a communication path for transmitting a request for authentication from said subscriber unit to said credential information manager;
 - a communication path for transmitting said transaction identifier from said subscriber unit to said credential information manager;
 - a communication path for transmitting a subscriber identifier from said subscriber unit to said credential information manager;

a computer program stored in said memory of said credential information manager for authenticating, by said credential information manager, said subscriber identifier received by said credential information manager from said subscriber unit with said subscriber identifier stored in said credential information manager memory;

a communication path for transmitting a request for verification from said credential information manager to said transaction service provider;

a communication path for transmitting, from said credential information manager to said transaction service provider, said transaction identifier received from said subscriber unit;

a computer program stored in said memory of said transaction service provider for verifying, by transaction service provider, said transaction identifier received by transaction service provider from said credential information manager with said transaction identifier stored in said transaction service provider memory;

a communication path for transmitting, from said transaction service provider to said credential information manager, a verification request result message;

a communication path for transmitting, from said credential information manager to said transaction service provider, said cyber identifier stored in said credential information manager memory;

a communication path for transmitting, from said credential information manager to said transaction service provider, said subscriber information stored in said credential information manager memory; and

a communication path for transmitting a transaction authorization from said credential information manager to said transaction service provider.

59. The system of claim 58 wherein said subscriber unit is made up of one or more mobile phones, smart phones, PDAs, computers, or POS terminals, modems, fax machines, or display/input terminals.
60. The system of claim 59 wherein said subscriber unit is made of a phone in wireless communication with a POS terminal.
61. The system of claim 58 where one or more of the communication paths include a secure telecommunications link.
62. The system of claim 58 where one or more of the communication paths include a wireless telecommunications link.
63. The system of claim 58 where one or more of the communication paths include the internet.
64. The system of claim 61 wherein said secure telecommunications link includes one or more of a VPN, audio or visual signalling, secure tunnelling, or an encrypted communication infrastructure.
65. The system of claim 58 wherein said subscriber unit memory includes a removable memory, and before said subscriber identifier is transmitted from said subscriber unit to said credential information manager, said subscriber identifier is stored in said subscriber unit memory.
66. The system of claim 65 wherein said removable memory includes a SIM card.
67. The system of claim 65 wherein said removable memory includes an electronic card.
68. The system of claim 58 wherein said credential information manager further includes:
a certified credential information manager having a processor and a memory,
an authentication/secure link service provider having a processor and a memory,
a communication path for transmitting said request for authentication, received from said subscriber unit by said credential information manager, from said

certified credential information manager to said authentication/secure link service provider,
a communication path for transmitting said subscriber identifier, received from said subscriber unit by said credential information manager, from said certified credential information manager to said authentication/secure link service provider,
wherein said authentication computer program is stored in said authentication/secure link service provider memory, and
wherein said subscriber identifier stored in said credential information manager memory is stored in said authentication/secure link service provider memory.

CLAIMS

1. A method for securing a transaction by a user comprising:

providing a subscriber unit having a processor, a memory, and a display,
wherein said subscriber unit is configured to accept user input,
providing a credential information manager having a processor and a memory,
storing a cyber identifier associated with the user in said credential
information manager memory, wherein said cyber identifier comprises a
username and subscriber information;
storing a subscriber identifier associated with the user in said credential
information manager memory;
storing said subscriber information associated with the user in said credential
information manager memory;
providing a transaction service provider having a processor and a memory,
transmitting a request for a transaction from said subscriber unit to said
transaction service provider;
transmitting a transaction identifier, created by said transaction service
provider based on said transaction request, from said transaction service
provider to said subscriber unit;
storing said transaction identifier in said transaction service provider memory;
transmitting a request for authentication from said subscriber unit to said
credential information manager;
transmitting said transaction identifier from said subscriber unit to said
credential information manager;
transmitting a subscriber identifier from said subscriber unit to said credential
information manager;
authenticating, by said credential information manager, said subscriber
identifier received by said credential information manager from said
subscriber unit with said subscriber identifier stored in said credential
information manager memory;
transmitting a request for verification from said credential information manager
to said transaction service provider;

transmitting, from said credential information manager to said transaction service provider, said transaction identifier received from said subscriber unit;

verifying, by transaction service provider, said transaction identifier received by transaction service provider from said credential information manager with said transaction identifier stored in said transaction service provider memory;

transmitting, from said transaction service provider to said credential information manager, a verification request result message;

transmitting, from said credential information manager to said transaction service provider, said cyber identifier stored in said credential information manager memory;

transmitting, from said credential information manager to said transaction service provider, said subscriber information stored in said credential information manager memory;

transmitting a transaction authorization from said credential information manager to said transaction service provider; and

transmitting a password from said subscriber unit to said transaction service provider;

wherein said password is never transmitted to said credential information manager and wherein said cyber identifier is never transmitted to said subscriber unit; and

wherein said subscriber information is never transmitted to said transaction service provider by said subscriber unit.

2. The method of claim 1 wherein said authentication further includes comparing, by said credential information manager processor, said subscriber identifier received by said credential information manager from said subscriber unit with said subscriber identifier stored in said credential information manager memory.

3. The method of claim 2 wherein said verification request is sent as a result of said comparison indicating that said subscriber identifier received by said credential information manager from said subscriber unit matches said subscriber identifier stored in said credential information manager memory.

4. The method of claim 2 further including transmitting an authentication failure message from said credential information manager to said subscriber unit, wherein said authentication failure message is sent as a result of said comparison indicating that said

subscriber identifier received by said credential information manager from said subscriber unit does not match said subscriber identifier stored in said credential information manager memory.

5. The method of claim 4 further including displaying a visual authentication failure message on said subscriber unit display based on said authentication failure message transmitted from said credential information manager to said subscriber unit.

6. The method of claim 1 wherein said verification further includes comparing, by said transaction service provider processor, said transaction identifier received by transaction service provider from said credential information manager with said transaction identifier stored in said transaction service provider memory, wherein said verification result request message includes a result of said comparison.

7. The method of claim 6 wherein said transmission of said cyber identifier is sent as a result of said verification result request message indicating that said transaction identifier received by said transaction service provider from said credential information manager matches with said transaction identifier stored in said transaction service provider memory.

8. The method of claim 6 further including transmitting a verification failure message from said credential information manager to said subscriber unit, wherein said verification failure message is sent as a result of said verification result request message indicating that said transaction identifier received by said transaction service provider from said credential information manager does not match with said transaction identifier stored in said transaction service provider memory.

9. The method of claim 8 further including displaying a visual verification failure message on said subscriber unit display based on said verification failure message transmitted from said credential information manager to said subscriber unit.

10. The method of claim 1 wherein said subscriber unit is made up of one or more mobile phones, smart phones, PDAs, computers, or POS terminals, modems, fax machines, or display/input terminals.

11. The method of claim 10 wherein said subscriber unit is made of a phone in wireless communication with a POS terminal.

12. The method of claim 1 where one or more of the transmissions are made via a secure telecommunications link.

13. The method of claim 1 where one or more of the transmissions are made via a wireless telecommunications link.

14. The method of claim 1 where one or more of the transmissions are made via the internet.

15. The method of claim 12 wherein said secure telecommunications link includes one or more of a VPN, audio or visual signaling, secure tunneling, or an encrypted communication infrastructure.

16. The method of claim 1 wherein, before said subscriber identifier is transmitted from said subscriber unit to said credential information manager, said subscriber identifier is received as input to the subscriber unit and stored in said subscriber unit memory.

17. The method of claim 1 wherein said subscriber unit memory includes a removable memory, and before said subscriber identifier is transmitted from said subscriber unit to said credential information manager, said subscriber identifier is stored in said subscriber unit memory.

18. The method of claim 17 wherein said removable memory includes a SIM card.

19. The method of claim 17 wherein said removable memory includes an electronic card.

20. The method of claim 1 further including storing said subscriber information, transmitted from said credential information manager to said transaction service provider, in said transaction service provider memory.

21. The method of claim 1 further including transmitting said subscriber information, transmitted from said credential information manager to said transaction service provider, from said transaction service provider to said subscriber unit.

22. The method of claim 21 further including displaying visual subscriber information on said subscriber unit display based on said subscriber information transmitted from said transaction service provider to said subscriber unit.

23. The method of claim 1, further comprising verifying, by said transaction service provider, said password transmitted from said subscriber unit.

24. A system for securing a transaction by a user comprising:

a subscriber unit having a processor, a memory, and a display,
 wherein said subscriber unit is configured to accept user input,

a credential information manager having a processor and a memory,

a cyber identifier associated with the user stored in said credential information manager memory, wherein said cyber identifier comprises a username and subscriber information;

a subscriber identifier associated with the user stored in said credential information manager memory;

said subscriber information associated with the user stored in said credential information manager memory;

a transaction service provider having a processor and a memory,

a transaction request configured to be transmitted by a communication path from said subscriber unit to said transaction service provider;

a computer program stored in said memory of said transaction service provider for creating, based on said transaction request, a transaction identifier;

said transaction identifier configured to be transmitted by a communication path from said transaction service provider to said subscriber unit;

said transaction identifier stored in said transaction service provider memory;

a request for authentication configured to be transmitted by a communication path from said subscriber unit to said credential information manager;

said transaction identifier configured to be transmitted by a communication path from said subscriber unit to said credential information manager;

a subscriber identifier configured to be transmitted by a communication path from said subscriber unit to said credential information manager;

a computer program stored in said memory of said credential information manager for authenticating, by said credential information manager, said subscriber identifier received by said credential information manager from said subscriber unit with said subscriber identifier stored in said credential information manager memory;

a request for verification configured to be transmitted by a communication path from said credential information manager to said transaction service provider;

said transaction identifier, received from said subscriber unit, configured to be transmitted by a communication path from said credential information manager to said transaction service provider;

a computer program stored in said memory of said transaction service provider for verifying, by transaction service provider, said transaction identifier received by transaction service provider from said credential information manager with said transaction identifier stored in said transaction service provider memory;

a verification request result message configured to be transmitted by a communication path from said transaction service provider to said credential information manager;

said cyber identifier, stored in said credential information manager memory, configured to be transmitted by a communication path from said credential information manager to said transaction service provider;

said subscriber information, stored in said credential information manager memory, configured to be transmitted by a communication path from said credential information manager to said transaction service provider;

a transaction authorization configured to be transmitted by a communication path from said credential information manager to said transaction service provider; and

a password configured to be transmitted by a communication path from said subscriber unit to said transaction service provider;

wherein said password is never transmitted to said credential information manager and wherein said cyber identifier is never transmitted to said subscriber unit; and

wherein said subscriber information is never transmitted to said transaction service provider by said subscriber unit.

25. The system of claim 24 wherein said subscriber unit is made up of one or more mobile phones, smart phones, PDAs, computers, or POS terminals, modems, fax machines, or display/input terminals.

26. The system of claim 25 wherein said subscriber unit is made of a phone in wireless communication with a POS terminal.

27. The system of claim 24 where one or more of the communication paths include a secure telecommunications link.

28. The system of claim 24 where one or more of the communication paths include a wireless telecommunications link.

29. The system of claim 24 where one or more of the communication paths include the internet.

30. The system of claim 27 wherein said secure telecommunications link includes one or more of a VPN, audio or visual signaling, secure tunneling, or an encrypted communication infrastructure.

31. The system of claim 24 wherein said subscriber unit memory includes a removable memory, and before said subscriber identifier is transmitted from said subscriber unit to said credential information manager, said subscriber identifier is stored in said subscriber unit memory.

32. The system of claim 31 wherein said removable memory includes a SIM card.

33. The system of claim 31 wherein said removable memory includes an electronic card.

34. The system of claim 24 wherein said credential information manager further includes:

- a certified credential information manager having a processor and a memory,

- an authentication/secure link service provider having a processor and a memory,

- said authentication request, received from said subscriber unit by said credential information manager, configured to be transmitted by a communication path from said certified credential information manager to said authentication/secure link service provider,

- said subscriber identifier, received from said subscriber unit by said credential information manager, configured to be transmitted by a communication path from said certified credential information manager to said authentication/secure link service provider,

- wherein said authentication computer program is stored in said authentication/secure link service provider memory, and

- wherein said subscriber identifier stored in said credential information manager memory is stored in said authentication/secure link service provider memory.

35. The system of claim 24, wherein said transaction service provider is configured to verify said password transmitted from said subscriber unit