

Claims:

1. A method of performing a financial transaction via unsecured public telecommunication infrastructure comprising the steps of:
 - collecting data relating to a specified financial transaction type;
 - 5 building a transaction token including collected data and/or data derived from the collected data;
 - encrypting the transaction token;
 - creating a financial transaction protocol message incorporating the encrypted transaction token as dependent on a selected transport
 - 10 channel through which the message is to be conveyed; and
 - conveying the financial transaction protocol message using the selected transport channel and by way of the unsecured public telecommunication infrastructure to a destination where the financial transaction protocol message will be further processed.
 - 15
2. A method according to claim 1, where the step of collecting data relating to a specified transaction type includes the sub-step of collecting authentication data which is thereafter encrypted and the transaction token built thereafter includes the encrypted authentication data.
- 20 3. A method according to claim 2, including the step of formatting the authentication data.
- 25 4. A method according to claim 1, where the step of collecting data relating to a specified financial transaction type includes obtaining data by at least one of the following ways: from files stored on a device used to obtain the data; from a data reader associated with, or integrated into, the device used to obtain the data; from a customer by way of the user interface of the device used to
- 30 obtain the data.

5. A method according to claim 1, where the step of collecting data relating to a specified financial transaction type includes obtaining a set of transaction rules applicable to the financial transaction type.
- 5 6. A method according to claim 1, further including the step of padding the transaction token as required for the selected transport channel.
7. A method according to claim 1, further including the step of calculating a session key, the session key then being used to encrypt the transaction token
10 during the step of encrypting the transaction token.
8. A method according to claim 1, where the selected transport channel is GPRS.
- 15 9. A method according to claim 8, where the step of creating a transaction token includes the sub-steps of:
 appending an end token record data value to the transaction token;
 and
 padding the transaction token with null values until the altered
20 transaction token is a multiple of 8 bytes.
10. A method according to claim 9, where the step of encrypting the transaction token further includes the sub-steps of calculating a message authentication code session key and encrypting the altered and padded transaction token
25 using the message authentication code session key.
11. A method according to claim 10, where the step of creating a financial transaction protocol message includes the sub-step of creating a key serial number and where the financial transaction protocol message so created
30 comprises the key serial number the transaction token and a message authentication code session key.
12. A method according to claim 1, where the selected transport channel is SMS.

13. A method according to claim 12, where the step of building the transaction token further includes the sub-steps of determining a padding counter and a message counter and appending the padding counter and the message counter to the message.
14. A method according to claim 13, where the step of encrypting the transaction token includes the sub-step of encrypting the transaction token using a ciphering key based on 3GPP TS 03.48 specifications.
15. A method according to claim 12 or claim 13, where the step of creating a financial transaction protocol message includes the sub-step of prefixing the encrypted transaction token with a SMS header.
16. A communications device for facilitating the performance of a financial transaction via unsecured public telecommunication infrastructure, the communications device operable to execute software stored thereon or on removable media in data and control communication with the device to:
- collect data relating to a specified financial transaction type;
 - build a transaction token including collected data and/or data derived from the collected data;
 - encrypt the transaction token;
 - create a financial transaction protocol message incorporating the encrypted transaction token as dependent on a selected transport channel through which the message is to be conveyed; and
 - convey the financial transaction protocol message using the selected transport channel and by way of the unsecured public telecommunication infrastructure to a destination where the financial transaction protocol message will be further processed.
17. A communications device according to claim 16, where collected data includes authentication data and where the transaction token includes the authentication data in an encrypted form.

18. A communications device according to claim 16, further including a reader for reading information stored on external devices.

5 19. A communication device according to claim 16, the communications device operable to communicate by way of one or more of the following transport channels: GPRS; SMS.

10 ~~20. A card comprising at least one integrated circuit, the card being of similar size and shape to ordinary SIM card where, when the card is received within a device having a SIM card interface, executable software stored on a memory means of the at least one integrated circuit, when executed, is able to communicate with software stored on the device thereby allowing the device to provide both SIM and PSAM functionality to a user of the device.~~

15 ~~21. A card according to claim 20, where the device is only able to be operated as a SIM or PSAM at any point in time and communication between the software stored on the memory means and software stored on the device is by way of a logical communications channel~~