

CLAIMS

1. A method of processing a transaction in a digital network using data strings to identify parties, the data strings having a prescribed format comprising first, second and third data fields and a checksum, whereby the value of first data field identifies an accrediting entity; the value of the second data field identifies an issuing entity acting as a settlement proxy for a customer; the value of the third data field identifies a customer; and the value of the checksum establishes the integrity of the data string, the method comprising the steps of:
 - providing a primary data string to a customer;
 - assigning an address space within the third data field for use by a further party acting with the authority of the customer, such that (i) all third data values within the assigned address space are available for use in creating valid data strings and (ii) valid data strings having third data values which lie within the designated address space are subordinate data strings to the primary data string within a data hierarchy;
 - establishing constraints subject to which transactions using a given subordinate data string may be conducted and identifying to the accrediting agency, by reference to a range of values lying within the assigned address space, a location within the network of those transaction constraints;
 - requesting a token having the prescribed data format and a valid checksum from the accrediting entity by submitting a token request that includes the given subordinate data string;
 - parsing the token request to identify the given subordinate data string and the location of the transaction constraints;
 - requesting the transaction constraints from the location; and
 - storing the transaction constraints at the accrediting entity.
2. A method according to claim 1 further comprising the step of receiving at the accrediting entity, a request for authorisation of a transaction, the request including the token and data expressing conditions of the requested transaction; and
 - comparing the transaction conditions to the transaction constraints and, where the conditions lie within the constraints, passing the transaction request to the issuing entity.

3. A method according to claim 1 or claim 2 wherein the subordinate data string identifies an authorised user acting with the authority of the customer, and the step of requesting a token is initiated by the authorised user.
4. A method according to claim 3 wherein:
 - the transaction constraints are constraints applying to use of the subordinate data string by the authorised user and the transaction constraints are held at the location by a trusted administrator; and
 - the trusted administrator retains network contact data relating to the authorised user of the subordinate data string.
5. A method according to claim 4 further comprising the step, following the step of requesting the transaction constraints from the location and prior to storing the transaction constraints at the accrediting entity, of the trusted administrator dispatching an authentication challenge to the authorised user using the contact data.
6. A method according to claim 5 further comprising the step of receiving response data from the authenticating challenge and in response thereto of sending the transaction constraints to the accrediting agency for it to store.
7. A method of authorising a payment token request to enable processing a transaction in a digital network using data strings to identify parties, the data strings having a prescribed format comprising first, second and third data fields and a checksum, whereby the value of first data field identifies an accrediting entity; the value of the second data field identifies an issuing entity acting as a settlement proxy for a customer; the value of the third data field identifies a customer; and the value of the checksum establishes the integrity of the data string, wherein a primary data string is provided to a customer; an address space within the third data field is assigned for use by a further party acting with the authority of the customer, such that (i) all third data values within the assigned address space are available for use in creating valid data strings and (ii) valid data strings having third data values which lie within the designated address space are subordinate data strings to the primary data string within a data hierarchy; constraints subject to which transactions using a given subordinate data string may be conducted are established and a location within the network of those transaction constraints is identified to the accrediting agency, by reference to a range of values lying within the assigned address space; a token having the prescribed data format and a valid checksum is requested from the accrediting entity by the submission of a token request that includes the given subordinate data string; the token request

is parsed to identify the given subordinate data string and the location of the transaction constraints; and the transaction constraints are requested from the location, wherein the subordinate data string identifies an authorised user acting with the authority of the customer, and the step of requesting a token is initiated by the authorised user;

the method comprises the steps, performed by a trusted administrator of:

- applying transaction constraints to use of the subordinate data string by the authorised user;

- retaining the transaction constraints at the location; and

- retaining network contact data relating to the authorised user of the subordinate data string;

- following the request of the transaction constraints from the location and prior to storing the transaction constraints at the accrediting entity, dispatching an authentication challenge to the authorised user using the contact data; and

- receiving response data from the authenticating challenge and in response thereto of sending the transaction constraints to the accrediting agency for it to store