CLAIMS

1. A stored value updater (SVU) network arranged to receive a request to update a plurality of stored value cards (SVCs), the SVU network comprising:-

(a) a plurality of SVU devices in encrypted data communication with an access network,

(1) wherein each SVU device is configured to receive a plurality of stored value update requests via contactless communication from the plurality of SVCs, each stored value update request related to one of the SVCs;

(2) wherein each SVC is associated with an SVC identifier; and

(3) wherein each stored value update request includes one of the SVC identifiers and a requested reload amount;

(b) an SVU manager comprising one or more servers in data communication with the plurality of SVU devices through the access network,

(1) wherein the one or more servers are in data communication with at least one first database;

(2) wherein the at least one first database includes a plurality of first records;

(3) wherein each first record is associated with one of the SVU devices and each first record includes a status for the SVU device associated with the first record; and

(4) wherein each SVU device is operable to be in data communication with the SVU manager using a user datagram protocol (UDP) based communication protocol; and

(c) a SVU hardware security module,

(1) wherein the SVU hardware security module is configured to, for each stored value update request, generate a related encrypted authentication request based on at least the SVC identifier of the stored value update request; and

(2) wherein, for each stored value update request, the related encrypted authentication request is encrypted based on at least a terminal session key before authentication of the SVC related to the stored value update request.

2. The stored value updater network according to claim 1, wherein the SVU hardware security module implements a Secure Access Module (SAM) functionality.