SUMMARY

[0012a] According to a first aspect, there is provided a method to authenticate a claimant comprising: receiving, from the claimant, at least one set of data that has been captured by the claimant from at least one spot beam transmission wherein the data comprises a pseudo-random number and a time stamp associated with the data; further receiving, from the claimant, at least one location identifier; comparing the location identifier and the at least one set of data to a known valid data set, including comparing the location identifier with a known location for the spot beam at a time corresponding to the time stamp; and authenticating the claimant when a difference between the claimant data and the valid data set is less than a threshold.

[0012b] According to a second aspect, there is provided an apparatus to authenticate a claimant, comprising: a processor; and a memory module comprising logic instructions which, when executed, configure the processor to operate in accordance with the first aspect.

[0012c] According to a third aspect, there is provided a system to authenticate a claimant, comprising: at least one signal source to transmit a spot beam in accordance with a known spot-beam geometry; at least one electronic device comprising a receiver to receive at least one set of data from the spot beam transmission wherein the data comprises a pseudorandom number and a time stamp associated with the data, wherein the at least one electronic device is able to determine its location; and at least one verifier communicatively coupled to the at least one electronic device to authenticate a claimant comprising the electronic computing device, wherein the at least one verifier comprises a processor and a memory module, the memory module comprising logic instructions which, when executed, configure the processor to: receive, from the electronic device, the at least one set of data that the electronic device captured from the spot beam transmission; further receive, from the electronic device, at least one location identifier determined by the electronic device; compare the location identifier and the at least one set of data to a known valid data set, including comparing the location identifier with a known location for the spot beam at a time corresponding to the time stamp; and authenticate the claimant when a difference between the electronic device data and the valid data set is less than a threshold.

[0013] Described herein are an apparatus, systems, and methods for spot beam based authentication. In one or more embodiments, a method to authenticate a claimant involves a satellite transmitting distinctive beam data via a spot beam, a claimant capturing said data from said satellite transmission, a claimant transmitting the data to a verifier which may include the use of a mediatory means of data transmission, the verifier then authenticating the claimant when the difference between the claimed data and the known valid data set is within a defined threshold. In one or more embodiments, the claimant is provided access to a system or resource once they have been authenticated via this "one-way" authentication method. In one or more embodiments, a third party verifier may complete authentication of the claimant for a host network. In one or more embodiments the claimant may have a device that is capable of both receiving data and transmitting data, whereas in alternative embodiments the two functionalities may be housed in separate pieces of hardware coupled together.

[0014] In one or more embodiments, the data may be invalidated and the clamant is denied access. In one or more embodiments, the data may be marked as uncertain and may require additional data to authenticate the claimant. In one or more embodiments, the data may be marked as uncertain based on assigned tolerance levels and may either be promoted to authenticated or demoted to restricted. In one or more embodiments the claimant may transmit additional identifiers to the verifier for use in authentication which may include one of the following: satellite identifying information, other claimant captured data or derived information including location identifiers (e.g. earth-based coordinates, etc.), time, a pseudo-random code segment (i.e. an