CLAIMS

1. A method of payload assurance for a payload X which is to be transferred across a network boundary via any of multiple predetermined Boundary Control devices, the method comprising:

at a first electronic entity, upon receiving a request:

providing an electronic Authorisation token for defining properties of the payload X to be transferred;

defining a Boundary control group located at the network Boundary comprising a plurality of Boundary Control Devices having dedicated permanent identity information associated with each of them;

determining an ephemeral ID array in dependence upon the permanent identity information of each of the Boundary Control Devices in the Boundary Control group and the Authorisation token; and

generating an electronic Release token in dependence upon the ephemeral ID array and the Authorisation token, to be forwarded to a second electronic entity, the release token being valid for use with the Boundary Control Devices provided in the defined Boundary Control Group.

2. The method of payload assurance for a payload X according to claim 1, the method further comprising generating at least one entropy element to form part of the electronic authorisation token for ensuring

that multiple electronic authorisation tokens authorising the same payload properties are unique.

3. The method of payload assurance for a payload X according to claim 1 or claim 2, wherein the Release token is applied to one or more payload transfer authorisation requests during a period of validity of the Release token.

4. The method of payload assurance for a payload X according to claim 3, wherein the period of validity of the Release token depends upon a predetermined time period defined in the Authorisation token by the first electronic entity.

5. The method of payload assurance for a payload X according to any preceding claim, wherein on receipt of the Release token and upon a payload transfer request the second electronic entity creates a File token for each Boundary Control Device in a gateway group dependent upon the ephemeral array, a Local token comprising parameters defined remotely from the first entity and a hash digest of the payload X to be transferred, so as to provide an array of File tokens $\{F_t\}$.

6. The method of payload assurance for a payload X according to claim 5, wherein the hash digest is provided by passing the payload X through a one-way function prior to the payload X being received by the second entity as a part of the payload transfer request.

7. The method of payload assurance for a payload X according to claim 5 or claim 6, wherein the Local token comprises an entropy element.

8. The method of payload assurance for a payload X according to any of claims 5 to 7, wherein at least one of the Local token parameters are provided by a third electronic entity for validating desired payload parameters for payload transfer across the Network Boundary.

9. The method of payload assurance for a payload X according to claim 8, wherein a fourth electronic entity acting as a payload sender entity and the sole electronic entity in contact with the Boundary Control Devices of the Boundary Control Group, defines at least one of the Local token parameters.

10. The method of payload assurance for a payload X according to claim 8 or 9 wherein the third electronic entity validates the payload against predetermined rules provided upon receipt of the payload transfer request and/or the intended payload transfer destination and provides an evidence object of the validation for inclusion in the Local token.

11. The method of payload assurance for a payload X according to any of claims 5 to 10, wherein the second entity is configured to subsequently generate a payload Header dependent upon the Authorisation token, the Local token, the file token array and the hash digest of the payload.

12. The method of payload assurance for a payload X according to claim 11, wherein the payload Header is prepended to the payload X prior to the payload X being forwarded by a fourth entity to one or more Boundary Control Devices in the Boundary Control group.

13. The method of payload assurance for a payload X according to claim 12, wherein upon at least part of the payload having payload Header E reaching a Boundary Control Device, the Boundary Control Device regenerates the Session ID $(S_i)_g$ using permanent ID information of the Boundary Control Device and the Authorisation Token from the payload Header.

14. The method of payload assurance for a payload X according to claim 13, wherein at one of the Boundary Control Devices, a Session ID is used, along with parameters within the payload Header to calculate a file token F_t'.

15. The method of payload assurance for a payload X according to claim 14, wherein F_t'= # (#(X), L, J, HMAC (K_G', A)) from the payload header, wherein the Session ID is HMAC (K_G', A).

16. The method of payload assurance for a payload X according to claim 14 or claim 15, wherein the Boundary Control Device compares the File token F_t' to the File token array located in the Header E to determine whether the File token is identical to a value in the File token array {F_t} and in a case that there is a match, subsequently generating a first positive event outcome identifier.

17. The method of payload assurance for a payload X according to claim 15 or 16, wherein the Boundary Control Device passes the payload through a one way function to provide $\#(X)_g$ from X and compares $\#(X)_g$ with #(X) of the Header E, and in the case that there is a match, subsequently generating a second positive event outcome identifier.

18. The method of payload assurance for a payload X according to claim 16 or 17, the Boundary Control Device further comparing other control criteria contained in an export or import header to ensure the control criteria are within predefined limits and in the case that it is, providing a third positive outcome identifier.

19. The method of payload assurance for a payload X according to claim 16, 17 and/or 18, wherein the Boundary Control device identifies a first positive outcome identifier, a second positive outcome identifier and a third positive outcome identifier and subsequently determines a positive boundary control outcome.

20. The method of payload assurance for a payload X according to claim 19, wherein the Boundary Control Device transfers the payload X having Header E through the Boundary Control Device and across a network/domain boundary in the case that a positive boundary control outcome has been met.

21. The method of payload assurance for a payload X according to claim 20, wherein the Boundary control device is configured to prohibit passage of the file across the network/domain boundary and/or enable the file to be dropped in the case that a positive boundary control outcome has not been met.

22. The method of payload assurance for a payload X according to any preceding claims, wherein the one or more Boundary Control devices of a Boundary Control Group blocks invalid export headers and non-

compatible payloads with valid headers in dependence upon the Authorisation token and the Ephemeral ID Array.

23. The method of payload assurance for a payload X according to any preceding claim, wherein the payload is split into chunks that are less than the maximum size available from the Boundary Control Devices in the Boundary Control group.

24. The method of payload assurance for a payload X according to claim 23, further comprising creating an array of Payload Headers, one for each of the chunks based on the Authorisation Token, File Token, Local Token and the Hash table of the Payload.

25. The method of payload assurance for a payload X according to claim 24, further comprising prepending chunk's Payload Header to the corresponding chunked Payload and forwarding a resulting signed payload chunks to one or more Boundary control Device in the Boundary Control Group.

26. A payload assurance system for a payload X which is to be transferred across a network boundary via at least one predetermined boundary control device, the system comprising a first electronic entity having at least one computer processor and at least one data storage device, the at least one data storage device comprising instructions operative by the at least one computer processor to:

generate an electronic Authorisation token for defining properties of the payload X to be transferred;

define a Boundary control group located at the network Boundary comprising at least two Boundary Control Devices having dedicated permanent identity information associated with each of them;

determine an ephemeral ID array in dependence upon the permanent identity information of each of the Boundary Control Devices in the Boundary Control group and the Authorisation token; and

generate an electronic Release token in dependence upon the ephemeral ID array and the Authorisation token, to be forwarded to a second electronic entity in the system, the release token being valid for use with the Boundary Control Devices provided in the defined Boundary Control Group.

27. The payload assurance system according to claim 26, wherein the electronic authorisation token further comprising at least one entropy element for ensuring that multiple electronic authorisation tokens authorising the same payload properties are unique.

28. The payload assurance system according to claim 26 or 27, comprising multiple separate and distinct electronic entities, comprising of at least one Authoriser entity, at least one Sender entity, at least one Signer entity, and at least one Payload validation entity.

29. The payload assurance system, according to claim 28, further comprising the Signer entity being configured to sign any number of payloads using the Release token during a period of validity of the Release token.

30. The payload assurance system according to claim 29, wherein on receipt of the Release token and upon receipt of a payload export request the Signer entity is configured to calculate a file token for each Boundary Control Device in the gateway group dependent upon the ephemeral array, a Local token and a hash digest of the payload to be transferred, so as to provide an array of file tokens $\{F_t\}$.
31. The payload assurance system according to claim 30, wherein the hash digest is provided by passing the payload through a one-way function prior to forwarding the payload X to the Signer entity.
32. The payload assurance system according to claim 30 or claim 31, wherein the Local token defines parameters associated with the payload, a payload transfer destination and/or as defined by the Sender entity.
33. The payload assurance system according to any of claims 30 to 32, wherein the Local token comprises an entropy element.
34. The payload assurance system according to any of claims 30 to 33, wherein the Local token parameters are provided by the payload validation entity and/or the Sender Entity.
35. The payload assurance system according to claims 32 to 34, wherein the payload validation entity is configured to validate the payload against predetermined rules of the requester and/or the payload destination and is configured to provide an evidence object of the validation for inclusion in the Local token.

36. The payload assurance system according to any of claims 30 to 35, wherein the Signer entity is configured to subsequently generate a payload Header dependent upon the Authorisation token, the Local token, the File token array and the hash digest of the payload.

37. The payload assurance system according to claim 36, wherein the header is prepended to the payload prior to being forwarded to one or more BCDs of the gateway group.

38. The payload assurance system according to any of claims 26 to 37, wherein the payload is split into chunks that are less than the maximum size available from the Boundary Control Devices in a Gateway group.

39. The payload assurance system according to claim 38, further comprising the Signer entity being configured to create an array of Payload Headers, one for each of the chunks based on the Authorisation Token, File Token, Local Token and the Hash table of the Payload.

40. The payload assurance system according to claim 39, further comprising the Signer entity being configured to prepend chunk's Payload Header to the corresponding chunked Payload and to forward resulting signed payload chunks to one or more Boundary control Device in the Boundary Control Group.

41. The payload assurance system according to claims 37 or 40, wherein on receipt of the payload at a Boundary Control Device, the Boundary control device is configured to regenerate the gateway session ID $(S_i)_g$

using the Boundary Control devices permanent ID information and the Authorisation Token from the Header.

42. The payload assurance system according to claim 41, wherein at the Boundary Control Device the Session ID is used, along with parameters within the Header to calculate a file token F_t'.

43. The payload assurance system according to claim 42, wherein F_t'= # (#(X), L, J, HMAC (K_G', A)) from the header, wherein the Session ID is HMAC (K_G', A).

44. The payload assurance system according to claim 42 or claim 43 wherein the Boundary Control Device has a comparator configured to compare the File token F_t' to the File token array located in the Header E to determine whether the File token is identical to a value in the File token array {F_t} and in a case that there is a match the comparator is configured to generate a first positive event outcome identifier.

45. The payload assurance system according to any of claims 43 to 44, wherein the Boundary Control Device is configured to pass the payload through a one way function to provide $\#(X)_g$ from X, and a comparator subsequently compares $\#(X)_g$ with #(X) of the Header, and in a case that there is a match, the comparator is configured to generate a second positive event outcome identifier.

46. The payload assurance system according to any of claims 43 to 45, the Boundary Control Device further comparing other control criteria contained in the export or import header to ensure they are within

predefined limits and in the case that it is, the comparator configured to provide a third positive outcome identifier.

47. The payload assurance system according to claim 44, 45 or 46, the Boundary Control device configured to identify a first positive outcome identifier, a second positive outcome identifier and/or a third positive outcome identifier and subsequently determining a positive boundary control outcome in dependence upon the first positive outcome identifier, the second positive outcome identifier and the third positive outcome identifier.

48. The payload assurance system according to claim 47, wherein the Boundary Control Device is configured to transfer the payload X through the Boundary Control Device and across a network/domain boundary in the case that a positive boundary control outcome has been met.

49. The payload assurance system according to claim 47, wherein the Boundary control device is configured to prohibit passage of the file across a network/domain boundary and/or enable the payload to be dropped in the case that a positive boundary control outcome has not been met.

50. The payload assurance system according to any of claims 28 to 49, wherein the at least one Sender entity is the sole electronic entity in communication with the at least one Boundary Control Device.

51. The payload assurance system according to any of claims 27 to 51, comprising a random number generator or pseudo random number

generator for providing the entropy element of the electronic Authorisation token and/or the Local token.

52. An export control system for a payload X which is to be transferred across a network boundary via at least one predetermined boundary control device, the system comprising a first electronic entity having at least one computer processor and at least one data storage device, the at least one data storage device comprising instructions operative by the at least one computer processor to:

generate an electronic Authorisation token for defining properties of the payload X to be transferred;

define a Boundary control group located at the network Boundary comprising at least two Boundary Control Devices having dedicated permanent identity information associated with each of them;

determine an ephemeral ID array in dependence upon the permanent identity information of each of the Boundary Control Devices in the Boundary Control group and the Authorisation token; and

generate an electronic Release token in dependence upon the ephemeral ID array and the Authorisation token, to be forwarded to a second electronic entity in the system, the release token being valid for use with the Boundary Control Devices provided in the defined Boundary Control Group.

53. A payload assurance system for assuring a payload for transfer from a lesser trusted network to a trusted network (or vice versa) for a payload X, the system comprising a first electronic entity having at least

one computer processor and at least one data storage device, the at least one data storage device comprising instructions operative by the at least one computer processor to:

generate an electronic Authorisation token for defining properties of the payload X to be transferred;

define a Boundary control group located at a network Boundary comprising at least two Boundary Control Devices having dedicated permanent identity information associated with each of them;

determine an ephemeral ID array in dependence upon the permanent identity information of each of the Boundary Control Devices in the Boundary Control group and the Authorisation token; and

generate an electronic Release token in dependence upon the ephemeral ID array and the Authorisation token, to be forwarded to a second electronic entity in the system, the release token being valid for use with the Boundary Control Devices provided in the defined Boundary Control Group.

54. A network comprising a payload assurance system for assuring a payload for transfer from a lesser trusted network to a trusted network (or vice versa),), the payload assurance system comprising a first electronic entity having at least one computer processor and at least one data storage device, the at least one data storage device comprising instructions operative by the at least one computer processor to:

generate an electronic Authorisation token for defining properties of a payload X to be transferred;

define a Boundary control group located at a network Boundary comprising at least two Boundary Control Devices having dedicated permanent identity information associated with each of them;

determine an ephemeral ID array in dependence upon the permanent identity information of each of the Boundary Control Devices in the Boundary Control group and the Authorisation token; and

generate an electronic Release token in dependence upon the ephemeral ID array and the Authorisation token, to be forwarded to a second electronic entity in the system, the release token being valid for use with the Boundary Control Devices provided in the defined Boundary Control Group.