Payload assurance at a Network Boundary

The invention is in the field of data assurance at a Network Boundary or Gateway, in particular to provide assurance of the suitability and authorisation for the transfer of a payload X having an associated Header H between networks of different trust via a gateway.

In a high trust network one of the most significant risks is the exfiltration of data to a low trust network causing a breach of confidentiality. The egress paths on a high trust network will be, in many cases, formed of a high assurance boundary control, such as a data diode.

Due to its status as the 'gatekeeper' for a high trust network any processes used by the boundary control must be of high assurance i.e. provides a control where there is a high certainty that the correct decision is made under all possible circumstances. The requirement for high assurance limits what is possible in the hardware boundary control. For example, highly complex data (or information) formats require complex algorithms and processes to assure them, and it is hard to achieve high assurance of the correctness of implementation of a complex algorithm. In addition, some information formats are ambiguous in specification and change over time, so keeping any algorithm both highly assured and up to date is impractical. This can even be evidenced when considering very simple control criteria relating to payload content where the criteria response is time varying, for example in the case of determining whether a specific sequence of bytes represents a valid Unicode character, the answer will vary depending on when the enquiry was made.

Public Key Infrastructure (PKI's) are typically used to facilitate secure

electronic transfer of data over a network. It is used when a more rigorous authentication method is required to confirm the identities of the parties involved and to validate the data to be transferred across a network/domain boundary. However, the multiple elements needed to manage the digital certificates and public key encryption requires regular configuration and updates to maintain the desired level of system security.

There is therefore identified a need for a cross domain payload assurance method and system which provides payload assurances relating to suitability of egress data at a cross domain boundary, and which is of an improved security, is appropriately authorised for cross domain transfer, provides ephemeral authorisation, is agile to time variations, and can provide centralised management control.

Accordingly there is thus provided a payload assurance system for a Payload X which having a Header H to be transferred across a network boundary via at least one predetermined boundary control device, the system comprising 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 provide an electronic authorisation token for authorising properties of the payload to be transferred, the electronic authorisation token comprising at least one entropy element for ensuring that multiple electronic authorisation tokens authorising the same payload properties are unique.

Therefore, the uniqueness of the entropy element ensures that all authorisation tokens are also unique even when they are implemented to

provide identical payload property authorisations. Consequently, this provides authorisation tokens that are always distinguishable and capable of being audited.

A boundary transfer assessment step is provided at the Network Boundary, for indirectly determining whether the payload possesses the Authorisation token. The Header is used to make this assessment at the Boundary Control device.

The payload may be in the form of a file having a payload X and a header H. For example, the file may comprise an export file having an export header, or an import file having an import header. Both are capable of being transferred across a network domain boundary and require file assurance and authorisation to be considered prior to any transfer of the payload of the file occurring. Alternatively, the payload may be streamed data with a Header prepended. The boundary control device may be any device located at the network domain boundary e.g. a gateway, and is typically physical hardware, for providing hardware security control. The gateway may therefore be an export gateway, an import gateway or a pair/multiple number of export and/or import gateways. Alternatively the payload may be streamed data having an associated Header H.

The authoriser entity is effectively a central service entity located on the trusted side of the network boundary. The authoriser entity is responsible for specifying (or controlling) the properties of payloads permitted to be transferred across the network boundary.

By using different authorised payload parameters at the authoriser entity there is no longer a requirement to perform a software patch or re-configuration

of the gateway at the network boundary to allow egress of different files or payloads.

Another feature of the authoriser entity may be that it has permanent identity information. This permanent identity information is a unique identifier which is of the form of a 32/128 byte number. The permanent identity information for the electronic entity may be identical to the permanent identity information associated with the predetermined gateway. This may be achieved by sharing the unique identifier value between the gateway and the authorising entity or providing it at the point of manufacture or commissioning.

A Sender entity is located between the Authoriser entity and the Boundary control device and acts as an authorisation intermediary between the authorising entity and the gateway. Specifically, it only needs to be a communicative intermediary and not necessarily positioned in an intermediate location. It is the Sender entity that requests for the payload transfer across the domain boundary (so may also be considered to be a payload/file transfer request entity). This intermediary positioning of the Sender entity provides a level of isolation between the 1. authorisation step at the authoriser entity and the 2. comparator step at the Boundary Control Device, i.e. the Boundary Control Device is isolated from i. the authoriser entity making the top-level payload/file property authorisation decision and ii. the factors that have enabled that decision. This therefore provides the ability to autonomously validate at the Boundary Control Device the permitted payload/file properties against the payload/file authorisation without the need to configure the Boundary Control Device with the authorised properties.

The Sender entity may have no sight of the Permanent Identifier information which is a secret value.

The authorising properties are the payload attributes or associated criteria that are allowed to pass from the trusted to untrusted network or vice versa.

The payload assurance system may comprise multiple separate and distinct electronic entities, comprising of at least one Authoriser entity, at least one Sender entity and at the least one Boundary Control Device. These entities are communicatively coupled. It is preferable for only a single Authoriser entity to be implemented which acts as a Central Authoriser entity.

The Authoriser entity may be configured to create an ephemeral identity for a predetermined Boundary Control Device using the electronic authorisation token and permanent identity information associated with the predetermined Boundary Control Device. Effectively, the system may generate short term tokens from long term permanent identity tokens. The tokens may allow additional characteristics of the payload to be assured by the gateway (e.g. size, type, age of file/payload, age of token) if so desired. The ephemeral identity may be created at the Authorising Entity. The Authorising Entity is the Central Service, which can be a single service (more common) or multiple Authorisation services may be realised (which provides a more complex arrangement). Each of these separate services may provide Authorisation tokens for different payload criteria, which may provide a failsafe.

Therefore, where there are multiple Boundary Control Devices a single device must be selected by the Sender and this selection will be included in the payload transfer request.

The permanent identity information for each Boundary Control Device in the system may be stored at the Authoriser entity.

In a first embodiment of the invention, the at least one Authoriser entity may be configured to transfer the ephemeral identity to the Sender entity upon request.

The Sender entity may be configured to create an export or import header in dependence upon the ephemeral identity to be forwarded to the Boundary Control Device.

It is important to reiterate that the system can be implemented on payloads coming into a trusted network as well as payloads being exported from the trusted network.

In a second embodiment of the invention, there may be further provided at least one Signer entity, wherein the Signer entity is located communicatively intermediate the at least one Authoriser entity and the at least one Sender entity, so as to prevent the at least one Sender entity from communicating directly with the Authoriser entity. Communicatively intermediate means that whilst the physical position of the Signer entity may not necessarily be located intermediate the Authoriser entity and the Sender entity, what is instead desired is that the Sender entity is prohibited from communicating directly with the Authoriser entity and instead passes the transfer request via the Signer entity. Similarly, the Signer entity is prohibited from communicating directly with the Boundary Control Device. In fact, the Signer entity is the sole electronic entity type in communication with the at least one Authoriser entity. This ensures that the Authoriser entity is disassociated from the Boundary control device. By applying this Sender

entity and Signer entity arrangement, there is a minimise risk of erroneous authorisations being carried out.

In contrast to the first embodiment, the Authoriser entity may be configured to transfer the ephemeral identity to the Signer entity upon request.

The Signer entity may be configured to create an export or import header in dependence upon the ephemeral identity and to subsequently forward it to the Sender entity.

In both the first and second embodiments of the invention the Sender entity is configured to append the export or import header to the payload to form an export payload and to subsequently transfer the export payload to the predetermined Boundary Control Device.

The export or import payload associated header may further comprise a local token defining local properties of the payload to be transferred.

The Authoriser entity may be configured to provide an ephemeral identity of the Boundary Control Device in dependence upon the electronic authorisation token and the permanent identity information of the predetermined boundary control device by implementing a one-way mathematical function. The authorisation token and the permanent identity may be concatenated prior to applying the mathematical function.

The one-way mathematical function may comprise a HMAC, having an associated secret key.

The secret key may comprise the permanent identity information for the predetermined Boundary Control Device. Therefore, there is a requirement for the Sender entity to specify the Boundary Control Device of interest from multiple

options. Alternatively, only a single Boundary Control Device may be provided and in such a case there is no selection step required.

Beneficially, the at least one Sender entity may be the sole electronic entity in communication with the at least one Boundary Control Device.

The Boundary Control device may comprise a comparator, the comparator being configured to, upon receipt of the payload to be exported or imported, identify the authorisation token in the export or import payload header and to create a comparator ephemeral identity in dependence upon the authorisation token and its locally stored permanent identity information.

The comparator may be configured to directly or indirectly compare the ephemeral identity generated at the at least one Authoriser entity with the comparator ephemeral identity generated at the at least one Boundary Control Device so as to determine whether they are the same.

The comparator may be further configured to compare other control criteria contained in the export or import header to ensure they are within predefined limits.

Therefore, at the gateway there may be a comparison of respective values between the local criteria and authorisation criteria providing the file/payload delivery outcome. The authoriser entity and the at least one predetermined gateway have knowledge of a shared key value enabling this local and authorised criteria comparison. Local information may comprise environment information or other criteria requests from the request entity.

Preferably, the comparator may be configured to determine a positive boundary control outcome in the case that

i. the ephemeral identity generated is the same as the comparator ephemeral identity; and

ii. the other export header control criteria are within the predefined limits.

Therefore, the positive boundary outcome arises only when the aggregate of the test criteria have been met. Specifically, we need F_t to agree which means that whilst the gateway doesn't know the Authoriser ephemeral ID i.e. the session key, computing F_t indirectly indicates that the Session ID is also agreed.

The Boundary Control Device may be configured to transfer the payload X having Header H through the Boundary Control Device and across a network/domain boundary in the case that a positive boundary control outcome has been met.

Additionally, the Boundary control device may be configured to prohibit passage of the Payload X and associated Header H across the network/domain boundary and/or enable the Payload X to be dropped in the case that a positive boundary control outcome has not been met.

This configuration may provide autonomous handling of the file/payload at the gateway (or other domain boundary device) for authorisation (or otherwise) of the transfer of the file/payload.

The e.g. gateway has no understanding of the meaning of any of the header values, instead it is instructed to calculate comparators for the header values and to perform a test against the headers. Certain criteria have already been applied to the factory settings of the gateway, which cannot be changed even by the authoriser entity. Therefore, the method of calculating the comparator 10 and

the testing step undertaken at the gateway enables it to perform a strong and reliable enforcement function.

The payload assurance system may further comprise a random number generator or pseudo random number generator for providing the entropy element of the electronic authorisation token. The random number generator or pseudo random number generator is located in the Authoriser entity. This unique quantity must be random or pseudo random and the value is placed in the payload/file header. For a practical implementation, the value should not be predictable in advance of the token creation.

The electronic authorisation token may be publicly known.

In a further aspect of the invention there is provided an export control system for transferring an export file having an export header and payload X across the Network Boundary comprising the payload assurance system according to any preceding claim.

For the avoidance of doubt, the file/payload to be transferred across comprises an export file/payload having an export file/payload header dependent upon the electronic authorisation token (and which is appended to the payload).

In an alternative aspect of the invention there is provided a computational device comprising a system for assuring a payload for transfer from a lesser trusted network to a trusted network (or vice versa) comprising any of the above-mentioned features.

In a further aspect of the invention, there is provided a network comprising a system for assuring a payload for transfer from a lesser trusted network to a trusted network (or vice versa) comprising any of the above-mentioned features.

In a further aspect of the invention there is provided a method of assuring a file/payload for transfer across a network boundary via a Boundary Control Device using a system comprising 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 processor, the method comprising providing an electronic authorisation token configured to authorise the payload to be transferred, the electronic authorisation token comprising at least one element relating to properties of the payload and at least one entropy element for ensuring that multiple electronic authorisation tokens authorising the same payload properties are unique. The Authorisation of the payload criteria is also provided and signed off by a separate entity to the Authoriser entity. This is either carried out by the Sender entity (in embodiment 1) or by the Signer entity (as per embodiment 2). The creation of the export header is effectively the signing process.

Where the system further comprises at least one Authoriser entity and at least one Sender entity configured communicatively intermediate the Authoriser entity and Boundary Control Device, the method may further comprise creating an ephemeral identity for a predetermined Boundary Control Device using the electronic authorisation token and permanent identity information associated with the predetermined Boundary Control Device.

The ephemeral identity of a predetermined Boundary Control Device may be provided in dependence upon the electronic authorisation token and permanent identity information of the predetermined boundary control device by implementing a one-way mathematical function.

The one-way mathematical function comprises a HMAC, having an associated secret key. The secret key may comprise the permanent identity information for the predetermined Boundary Control Device. Effectively this is the Boundary Control Device that is of interest. Alternatively, a Hash function may be applied.

The method may further comprise storing the permanent identity information for each Boundary Control Device in the system at the Authoriser entity.

Beneficially, the permanent identity information may be prohibited from being accessed by the Sender entity.

The Authoriser entity may transfer the ephemeral identity to the Sender entity upon request, the Sender entity subsequently creating an export or import header in dependence upon the ephemeral identity.

The system may further comprise a Signer entity and the method may comprise the Authoriser entity transferring the ephemeral identity to the Signer entity upon request, the Signer entity may subsequently create an export or import header in dependence upon the ephemeral identity and may then subsequently forward the export or import header to the Sender entity. For the avoidance of doubt an export file/payload is created having an export file/payload header dependent upon the electronic authorisation token.

Creation of the header for the payload X, enables the checking of the payload header content against both the payload, environment information (e.g. time) and internal information of the gateway (e.g. pre-configured factory settings or the identity of the gateway). It is only once all of the tests are passed

that the payload is released by the gateway i.e. transferred from the trusted network to the lesser trusted network across a network boundary.

The method may further comprise providing the ephemeral identity of the predetermined Boundary Control Device in the export or import header.

The method may further comprise appending the export or import header to the payload at the Sender entity so as to create an export or import file/payload respectively and subsequently forwarding the export or import file/payload to the predetermined Boundary Control Device.

The method further may comprise providing local properties of the payload to be transferred in the export or import header.

At least part of the file/payload header beneficially comprises the hash generated by the hash function.

Upon receipt of the export or import file/payload at the Boundary Control Device the method may further comprise identifying the authorisation token in the export file/payload header; and creating a comparator ephemeral identity in dependence upon the authorisation token and the permanent identity information locally stored at the Boundary Control device.

It is necessary for the permanent identity information for the electronic entity to be identical to permanent identity information of the predetermined Boundary Control Device. If it is not, then the Boundary Control Device will not permit passage of the export file/payload.

The method may further comprise directly or indirectly comparing the ephemeral identity generated at the Authoriser entity with the comparator ephemeral

identity generated at the Boundary Control Device to determine whether they are identical.

The comparator may be further configured to compare other control criteria contained in the export header to ensure they are within predefined limits.

The method may further comprise determining a positive boundary control outcome in the case that

i. the ephemeral identity generated at the Authoriser entity is the same as the comparator ephemeral identity generated at the Boundary Control Device; and

ii. the other export header control criteria are within the predefined limits.

The file having payload X may be transferred through the Boundary Control Device and across a network/domain boundary when the positive boundary control outcome has been met.

Passage of the file may be prohibited and/or dropping of the file payload X may be enabled in the case that a positive boundary control outcome has not been met.

The method may comprise randomly or pseudo randomly generating a value to provide the entropy element of the electronic authorisation token. For example, a lava lamp bubble approach may be implemented to provide random numbers, or a pseudo random number generator may be applied instead.

The method may comprise determining the electronic authorisation token lifetime to be $T_{S1} \leq T_t \leq T_{S2}$ such that the authorisation is determined to be valid for the electronic authorisation token lifetime.

The method may comprise determining an export time period as $T_{M1} \leq T_t \leq T_{M2}$ such that the export of the file/payload is only permitted when the export period is satisfied.

The method may comprise calibrating and/or agreeing a time reference between the Authoriser entity and the at least one predetermined Boundary Control Device.

Once the properties of the payload are authorised through issuance of the Authorisation Token there is no option to change the authorised payload properties. This means that the boundary control device is not required to have any knowledge of the details of the validation scheme, but rather the inter-relationship between entities in the scheme e.g. the gateway only considers checkable assertions between the headers, intrinsic properties of the payload (e.g. size), the environmental factor (e.g. time limits). This allows for the use of sealed for life gateways to make release decisions autonomously. Autonomous in this instance means decisions are made without reference to other electronic entities. This maintains isolation (or separation) of the authorisation (at the CRA) and verification decision at the gateway and prevents the need for requesting the authentication decision from an alternative electronic entity, improving the security at the gateway by eliminating the ability for this decision information to be tapped by a third party. The boundary device can therefore comprise the simplest possible device that never requires replacement or updates and which never changes.

Only authorised payloads/exports may be allowed to be transferred across the domain boundary. A good export scheme usually considers: control of content, is time limited and ultimately stops the passage of unauthorised formats. Beneficially, the system may be configured to control the authorisations with an electronic token.

Computational devices may comprise a desktop or laptop computer, tablet, personal digital assistant (PDA), mobile phone, smart watch, hard disc, solid state disc or drive, memory, or other smart or mobile device capable of storing and/ or displaying data or otherwise acting as a data device, or a display device comprising a monitor, projector, screen or the like, capable of storing and/ or displaying data or otherwise acting as a data device are also disclosed, which may individually and/ or collectively comprise a device as outlined above for the user's convenience.

"File" is formed of a header H and a payload X. But it must be noted that the file assurance system and method can be used on Packets of data that also include an associated header and a payload, and also for streaming data where the export header is prepended before the streaming data.

Whilst the invention has been hereinbefore described it extends to any inventive combination of the features set out above, or in the following description, drawings or claims. For example, any features described in relation to any one aspect of the invention is understood to be disclosed also in relation to any other aspect of the invention.

The invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Figure 1 is a schematic of the system for a payload assurance at a network domain boundary in accordance with a first aspect of the invention;

Figure 2 shows a flow diagram of the method of payload assurance at the network boundary in accordance with a first aspect of the invention;

Figure 3 shows a representation of the Authorisation Token;

Figure 4 shows a representation of the Release Token;

Figure 5 shows a representation of the Export Header; and

Figure 6 shows a schematic of the system for payload assurance at a network domain boundary including a Signer entity.

In the Figures like elements are denoted by like reference numerals. The skilled reader will appreciate how complex the implementation of the method is, and thus the number of the optional features present, will be driven by the user requirements.

Referring to Figure 1, there is provided a payload authorisation control system 1 for a file having payload X which is to be transferred across a network boundary 2 via a Boundary Control Device G 3 (e.g. a Network Gateway formed of hardware), the system comprising a computer processor 4 and a data storage device 5. The system 1 and associated method provides for an immutable hardware boundary control for use in, for example, an Export Gateway and which assures that the export payload satisfies the following criteria:

- has undergone an approved assurance process;
- the format and content is unchanged in form after undergoing the assurance process;
- is compatible with the authorisation it is released under;

- has an unchanged name;
- can be uniquely identified (even if it is an identical copy of another payload);
- has authorisation that can be uniquely identified (even if identical to another authorisation);
- guarantees the authorisation to be unchanged from the point of provisioning to the entities involved in the release of the file.
- ensures separation of the roles of the scheme is enforced whenever the scheme is implemented.

For the file assurance scheme to operate there are several roles or entities that must undertake specially allocated functions. These entities comprise the following:

- The Sender 6: This entity requests authorisation appropriate to its role that allows it to create export headers for approved payloads, each of which it sends to the Network Boundary Device 3 e.g. a Gateway- either autonomously on its own behalf or acting on behalf of another entity, e.g. the Requester (not shown);
- The Requester (not shown): this optional entity is an external entity to the Export Authorisation control that desires to send a payload across a selected Gateway 3;
- The Central Release Authority (CRA) 7: this entity manages access to the Gateway identity blocks and creation of the authorisation upon enquiry by a Sender;
- The Export Gateway 3: This entity possesses a unique Identity Block and

will prohibit passage of i. any file that has an invalid export header and/or ii. any file that is not compatible with the export header even when the export file is valid.

In a first embodiment of the invention, the Authorisation Control and Assurance System 1 (hereafter referred to as the Authorisation System) is configured to provide authorised payload export for a single predetermined gateway 3. The Authorisation Scheme (which includes checks to be undertaken at the Gateway itself) allows some intrinsic properties of the payload (e.g. size) to be controlled, asserted properties (e.g. classification) to be compared, administrative features to be added, as well as enabling the lifetime for the authorisation to be managed via an electronic token. The scheme creates and utilises payload specific Export Header comprising three independent sub-tokens prepended to a specific payload. Only if the information in the Export Header is assurable as valid will the payload successfully obtain passage through the export Gateway 3 as requested by the Sender 6.

The Export Header and its component parts have two manifestations – an information representation (such as may be contained in a human readable JSON or XML file) and a binary representation which is a byte-level representation of how they are encoded in the Export Header for use in the functions underpinning the scheme. For simplicity both representations will be denoted by “token” (e.g. “authorisation token”) and the form of the token (information or binary) will be made explicit when significant.

The data storage device 5 comprises instructions operative by the processor 4 to provide an Authorisation Token A_t which will be described in more

detail. This provides a single level of signing by an authorised entity that can be consistently applied to various export authorisation requests.

The Authorisation Scheme requires the four electronic entities (or roles) introduced previously (or three roles if the Requester entity is in fact the Sender entity). The Export Gateway is a predetermined Boundary Control Device 3 located at a network domain boundary 2 i.e. located at a position enabling passage between a first network 8 and a second network 9 (or vice versa depending on whether export or import of the payload is required).

The Requester Entity (not shown) initiates the scheme by sending a request for the Sender entity 6 to send an export file through a predetermined Boundary Control Device 3 positioned at a network boundary 2.

The Sender entity 6 creates a Local Token L_t for the export file and creates a File Token F_t by combining L_t with the payload X, and the Release Token R_t. The Local Token L_t contains details about specific properties of the payload including:

- Nonce- which is used to disambiguate otherwise identical payloads;
- Information about itself e.g. UUID, original hash;
- Time limits- provision of 'not valid before' or 'not valid after' time thresholds, so as to prevent 'stale' payloads from being exported.
- Classification – an assertion of the classification of the payload.

The Sender entity 6 is also configured to i. create an Export Header by combining A_t, L_t and F_t, ii. sign the payload by combining the Export Header with the payload, and iii. send the signed payload to the predetermined Gateway 3. The Sender entity 6 will only be authorised to export files that satisfy

predetermined file criteria.

The CRA 7 acts as an authorising entity whereby it provides a Release Token R_t which is a unique token generated upon the Sender entity 6 enquiry. The CRA 7 predominantly holds the Boundary Control Device Permanent Identifier and is responsible for generating Session ID's S_i from Gateway Keys and Authorisation tokens A_t. The Session ID's are moderately sensitive, ephemeral values (or ephemeral identities) which expire regularly so pose no long-term risk. The Authorisation Token A_t and the Session ID S_i are forwarded as a pair as a response to the Sender entity 6 enquiry. This pair defines a Release Token.

The Sender entity 6 requests a Release Token from the CRA and creates an Export Header in dependence upon the Release Token for payloads it requires to authorise for export.

The Authorisation token created by the CRA 7 is an electronic token formed at least of a first part relating to authorised properties of the file and a second part for providing entropy (or randomness) to the token, therefore A_t=<entropy element> and <centrally specified parameter values>. The Authorisation token contains details about what the CRA 7 Authorises to be passed over a designated or predetermined Gateway 3 and also information about the Authorisation token itself, including its validity period. The entropy part is provided to ensure that multiple Authorisation Tokens authorising the same file properties are each unique. This enables for the specification of properties and associated authorisations to be centrally controlled and ensures that each authorisation request and associated response is distinguishable and as such auditable. In this embodiment the file is an export file to be transferred between

a trusted network 8 and a lesser trusted network 9 across a predetermined Boundary Control Device 3 e.g. Gateway G.

This Permanent Identity Information e.g. Identity block or other Key type associated with the Boundary Control device is highly sensitive information and must be stored very securely. The Permanent Identity information will hereafter be referred to as the Permanent ID of the predetermined Boundary Control Device 3 and denoted K_G.

Permanent Identity Information (K_G) related to the select Boundary Control Device 3 for the file transfer must be exclusively shared between the CRA 7 and the select Boundary Control Device when that device is brought into service. The select Boundary control device may i. have a K_G created at manufacture that is presented securely to the CRA, ii have a K_G created by the CRA loaded onto it, iii have a K_G created by an independent source loaded onto it and this same K_G loaded onto the CRA.

The Authorisation token can be mapped to a set of numerical values and used in the one-way functions described below. Provided all parts of the Export Control system use the same mapping the specifics of the mapping are not significant. The Authorisation token is a component of the Export Header to be provided to the Sender entity 6.

For the avoidance of doubt, the Authorisation Token contains the central Authorisation Controls which are assertions of what is permitted to be exported across the Boundary Control Device 3 for example, these may include:

- Version number;
- Entropy (to assure uniqueness of each Authorisation Header);

- Time limits- provision of 'not valid before' or 'not valid after' so as to control the lifetime of the token;
- Size- the maximum size (in bytes) of the payload (zero meaning no limit);
- Type- BMP, or other defined suitable file types as required, or any file type.

The Release Token R_t, which includes the Authorisation Token and the Session ID, is created by the CRA 7 and given to the Sender entity 6 and is used in the generation of every export payload header until its validity period expires or it is replaced by an updated Release Token upon a subsequent request from the Sender 6 to the CRA 7 . It is only the entropy element that ensures a unique response to each Authorisation Token request.

The Release Token R_t authorises the Sender to send payloads. It is not a payload specific authorisation and any number of payloads can be signed using the Release Token R_t during its period of validity.

The CRA 7 creates the Authorisation Response, by firstly providing an intermediate value in the form of a Session ID, which is obtained by combining the Authorisation Token and the selected Gateway Permanent ID K_G using a one-way mathematical function i.e. $S_i = f(K_G, A_t)$, where

- S_i is the session ID for a specific Boundary Control device;
- K_G is the Permanent ID for the specific gateway; and
- A_t is the authorisation token (in byte format).

For the avoidance of doubt, the session ID is created in the CRA and the one-way mathematical function f is compatible with the predetermined Boundary Control Device selected for the file transfer.

For this example of the invention, the one-way mathematical function may comprise an HMAC function, wherein the associated secret key is formed of the Permanent ID of the Boundary Control Device known by the CRA i.e. S_i = HMAC(K_G, A_t).

Alternatively, this one-way mathematical function comprises a Hash, wherein the associated secret key is formed of the Permanent ID of the Boundary Control Device K_G known by the CRA i.e. S_i=#(K_G, A_t).

The underpinning cryptographic hash function of either of these functions is not significant and any cryptographic hash function may be used. Selection of a suitable cryptographic hash algorithm by an implementor would be motivated by, amongst other things, consideration of algorithm longevity and cryptographic strength.

The step of generating S_i effectively creates an ephemeral identity which is derived from the shared Permanent ID and which is used by the Sender Entity 6 when forwarding the file for transfer across the network boundary, thereby alleviating the need to send the Permanent ID value. The Permanent ID remains an unknown value to the Sender entity 6 (i.e. it is effectively a secret value that is not known by the Sender entity 6 or the original, and external, Requester).

Upon a valid request from Sender entity 6 to use export gateway G the CRA 7 will calculate the HMAC and return the Releasee Token R_T= (A_t, S_i) to the Sender Entity 6. The HMAC calculation used to create S_i will be recreated at the gateway to assure that the associated A_t must be genuine as shall be discussed later.

For the sake of brevity, we suppose in each example below that the Sender Entity 6 is currently authorised to use a specific Boundary Control Device. If the Sender is currently authorised to use the Boundary Control Device, then it has no need to contact the CRA for an additional authorisation.

When in possession of R_t, the Sender entity generates a File Token F_t as follows:

$F_t = g(X, L_t, S_i)$.

The function g is compatible with the predetermined Boundary Control Device selected, but the function g need not be the same function type as the before mentioned function f. In this example, g is a hash function such that $F_t = \#(X, L_t, S_i)$ where the # denotes the hash as is the standard meaning in the art.

Other parameters such as payload name can be added to the hash provided the Boundary Control Device also has access to these parameters if the parameters are required to be used in an authorisation decision by the Boundary Control Device.

For example, to create the File Token F_t for a payload the Sender entity 6, upon being requested to sign payload X will calculate:

$$F_t = \# (X, L_t, J, S_i)$$

where

- X is the byte steam of the payload
- L_t is the Local Token (in byte format)
- J is the file name (in byte format)
- S_i is the session ID (in byte format)
- # denotes a suitable hash function also available to the

boundary control device.

The File Token F_t as created above is used in conjunction with the A_t and L_t tokens to create the Export Header for the payload as follows:

$$E = A_t \,||\, L_t \,||\, F_t$$

Finally, the signed payload file that is to be sent to the Boundary Control Device 3 is created at the Sender entity 6 by prepending the Export Header E to the payload X giving a signed export payload:

$$P = E \,||\, X$$

The signed export payload is then forwarded to the predetermined Boundary Control Device 3.

At the Boundary Control Device 3, comparisons are made between the file properties and the pre-set Boundary Control Device parameter criteria. Additionally, compliance checks are made against the file properties CRA 7 prescribed parameter criteria which form part of A_t.

The Boundary Control Device 3 holds its key and is configured to check the signed payload by checking that it was directed as intended and to check that the payload is compatible with the Local token and the Authorisation token. To ensure that the CRA 7 prescribed parameters are indeed authorised parameters they are only accessible when the Boundary Control Device 3 has undertaken a variety of authorisation criteria checks. The most important criteria to be achieved being provided by regenerating the session key (or ephemeral identity) S_i at the Boundary Control Device 3 by using the value of A_t received from the Sender Entity 6 (i.e. Header 1) and the Boundary Control Device local permanent identity information ID (which as mentioned previously is configured

to be identical to that used by the CRA 7). Assuming the Release Token R_t provided by the Sender entity 6 and the Release Token created at the Boundary Control Device 3 provide identical results, the parameters are determined to be validly authorised and payload compliance checks are made at the Boundary Control Device.

The Boundary Control Device 3 has a comparator 10 configured to undertake a simple comparison test of the file payload content against both the CRA specified parameter criteria and internal criteria specified at the Boundary Control Device (which are pre-configured factory settings).

Importantly, the CRA provides the 'critical' file criteria and these conditions must be met in order to validly authorise the payload to be transferred across the network domain boundary.

It is only once all of these tests are undertaken that the comparator 10 is able to determine a file delivery outcome to be applied. For example, the file is released by the Boundary Control Device 3 i.e. transferred from the trusted network 9 to the lesser trusted network 10 across a network boundary 2 if all of the test criteria have been met. If any of the test criteria flag a failure, then the file with payload X will not be permitted to pass through the Boundary Control Device 3 between the trusted network 8 and the lesser trusted network 9. Therefore, there is no transfer of the payload of the file across a network domain boundary in this instance.

In the case that the Release Token R_t provided at the Boundary Control Device is not identical to that produced by the Sender entity 6, there is no permission for the Boundary Control Device to access the specified parameters

and there is no authorisation obtained for transfer of the file between the trusted network and lesser trusted network via the Boundary Control Device.

This conditional criteria check effectively enables the intrinsic properties as specified by the CRA 7 to be autonomously assured by the Boundary Control Device 3.

As an alternative check and a way of indirectly checking the session key S_i, the export Gateway also has access to its K'_G then can calculate F_t'. Provided $F_t = F_t'$ then the gateway 3 can be confident that all elements used in the calculation are genuine, and can use the values to check the payload authorisation against other release constraints (time, type, size).

In this embodiment, the Sender Entity inserts additional local file property criteria which may be the same type (e.g. a time constraint) or a different type (e.g. a nonce) to those specified by the CRA 7 via the Local Token. This allows for the Sender Entity 6 to place additional constraints on the payload release decision which occurs at the Boundary Control Device.

The File Token F_t therefore becomes $\#(X, L_t, S_i)$ and Export Header is then provided by $(A_t || L_t || F_t)$. Once again, the Export Header gets prepended to the payload X before being forwarded from the Sender Entity to the Boundary Control Device. Therefore, a file header is created for use with the file payload X to be exported, wherein, at least part of the Export Header comprises the File Token F_t.

The comparator 10 is this time configured to undertake a simple comparison test of the file header content against both the file, environment information

(e.g. time) and internal information of the gateway (which are pre-configured factory settings or the identity of the gateway). For the avoidance of doubt, it is only once all of these tests are undertaken that the comparator 10 is able to determine a file delivery outcome to be applied. For example, the file is released by the Boundary Control Device 3 i.e. transferred from the trusted network to the lesser trusted network across a network boundary if all of the test criteria have been met. If any of the test criteria flag a failure, then the file with payload X will not be permitted to pass through the gateway between the trusted network and the lesser trusted network. Therefore, there is no transfer of the file and its payload across a network domain boundary in this instance.

This further embodiment effectively enables intrinsic properties to be autonomously assured by the Boundary Control Device and the same autonomous assurance can also be applied to the Local Token L_t properties.

The assurance of the authorisation parameters may be further strengthened by providing the Authorising Token A_t and Local Token L_t as a series of paired constraints and assertions (respectively) that are compared against each other using the comparator function located at the Boundary Control Device.

Specifically, the Boundary Control Device comparator 10 undertakes a comparison of respective values between the Local Token L_t which specifies local criteria and the Authorising Token A_t which is the Central Service authorised parameters.

It is reiterated that importantly the CRA 7 has knowledge of the unique Permanent ID associated with a pre-determined gateway that is to export the file

payload X and that the Sender Entity 6 has an ephemeral ID and does not know the Permanent ID of the Boundary Control Device 3. The Permanent ID is effectively a secret key value that is dependent upon the identity of the predetermined gateway.

In a yet further embodiment of the invention, the CRA 7 provides an Authorisation Token A_t that contains additional information which is not to be used in the release assurance or authorisation of the file, but is instead to be used to ensure the efficient management of the scheme. For example, A_T may contain a reference to the intended gateway of the signed payload to allow network and information routing entities to direct the signed payload to the correct gateway over a typical enterprise network.

The Boundary Control Device 3 is configured to check that data sent to it has been authorised by the CRA 7. In the case that the data is authorised and compatible with predetermined criteria (stored within a data file header prepended to a data file to be released) the file is transmitted. If the check determines that the data is not authorised or not compatible with the file header, the Boundary Control Device drops the file.

A random number generator 11 is used by the CRA 7 to provide the entropy element of the Authorisation Token A_t. The permanent ID information is stored in a secured storage area 11 in the CRA. Alternatively, a pseudo random number generator 11 may be used.

In use, there is provided a method of assuring a payload for transfer across a network boundary via a Boundary Control Device 3 using the here-before described system.

The method, which can be instigated by an external Requester Entity (not shown) is initiated by the Sender entity 6 requesting authorisation from the CRA 7 to transfer files across the at least one predetermined Boundary Control Device 3. The file has payload X. The CRA 7 issues a Release Token R_t to the Sender Entity 6.

The Authorising Token A_t is unique and is used to create an ephemeral identity that is used to create a Release Token R_t which is forwarded to the Sender Entity 6 as a response to a file transfer authorisation request. The Sender entity 6 creates an export header dependent upon the electronic authorisation token using a one-way function. The Sender entity 6 then prepends the export header to the payload X to form a signed export file and then forwards the signed export file to the Boundary Control Device 3. The Boundary Control Device 3 then compares content in the header to known local values hard programmed in the Boundary control device and to the authorised parameters specified by the CRA 7.

The Boundary Control Device 3 stores the Permanent ID and is configured to access it internally/locally to enable the computation of various functions. As mentioned previously, a copy of each Boundary Control Device secret is lodged with the CRA 7. The Permanent ID is determined at the time of manufacture of the gateway and is never changed and is of size 32 bytes. The Permanent ID is used to generate the Session ID S_i which is to be included in the Request Token T_t for issuance to the allowed Sender Entity. This allows the Sender Entity to egress the signed file via the preferred and predetermined gateway. The objective is for the Sender Entity 6 to produce an Export Header comprising a File Token

and an Authorising Token, that is to be sent with the Payload X to the Boundary Control Device 3.

The CRA 7 generates a 32 byte random value to be embedded in the Authorising Token so as to provide an Authorisation Token that is unique per request. For the token request to be a valid step, the Sender entity 6 must request values for the time constraints T_{S1} and T_{S2}, the maximum file size S and the file type F that are permitted by the CRA, or the CRA can impose predetermined values for any or all of these fields. There are two ways of achieving this: either the Sender can ask for values and the CRA 7 agrees, or the Sender entity requests “use gateway” and the CRA 7 mandates specific values.

In all cases the CRA 7 response includes the following parameter assertion information:

V: which is a version parameter to ensure that the predetermined gateway is compatible with the header. This is a simple one up number starting with 1.

S: which is the maximum file size in bytes for a file to be transferred across the gateway for that particular authorisation token. This is a 4 byte parameter where a value of 0 adopts the gateway maximum size.

F: which is the file type and has a size of 4 bytes. 0x0==any, and 0x1=BMP.

T_{S1}, which is of 4 bytes, is the Intermediate Value ‘valid from’ time in epoch time. An export must not be accepted if the epoch time is before this value.

T_{S2}, which is of 4 bytes, is the Intermediate Value ‘valid to’ time in epoch time. An export must not be accepted if the epoch time is after this value. The Intermediary Value I_v may instead be considered to be a session ID.

These values are combined into the A_t in the structure shown in Figure 3

Taking the SHA-256 HMAC of A_t with the Key of K_g

S_i=HMAC (K_G,A_t);

creates a new 32 byte value S_i. This is combined with A_t to give the Release Token R_t in the structure shown in Figure 4.

The first 96 bytes of this structure is the electronic Authorisation Token A_t which is re-used in this scheme and which is publicly known. The full 128 byte structure of the Release Token contains the intermediary value, Session ID, S_i.

File Type F checking criteria can be set at the Boundary Control Device and can determine whether a file meets the specification of a particular type. For example, the Bitmap format has a common format that consists of a BMP header and pixel array. Each of the entries in the header have known good value ranges, and that the size of the pixel array matches the declared size in the BMP header. The Boundary Control Device can be configured to check that if the file type is set to BMP then the payload complies with the BMP specification as implemented in the Boundary Control Device's checking criteria. Multiple file types can be set in a predetermined Boundary Control Device.

On possession of the Release Token containing the Authorisation Parameters and following the request to export a file the Sender entity generates a Local Token L_t which includes the following parameter assertion information:

N: a Nonce of size 4 bytes.

T_{M1}, which is of 4 bytes, is the 'useful from' time in epoch time. An export must not be accepted if the epoch time is before this value.

T_{M2}, which is of 4 bytes, is the 'valid until' time in epoch time. An export must not be accepted if the epoch time is after this value.

As well as the T_{S1} and T_{S2} provided by the CRA 7 in the Authorisation Token, there is provided the T_M pair by the Sender Entity 6 in the Local Token. The Session ID S_i validity window (based on the T_S times) may be measured in days and any payload arriving at the Boundary Control Device between the T_S time limits will be considered to have a valid A_t with respect to time. However, for some applications messages may have a useful lifetime of much less than the Authorising Token A_t token lifetime. To allow for messages to be rejected by the Boundary Control Device 3 when no longer useful (as opposed to not allowed) then the T_M times are used to define a "useful operational window" for messages and therefore act as a second time filter. Therefore, T_{M1} can be considered to be a signed file 'valid from' time in epoch time, whereby an export must not be accepted if epoch time is before this time. Similarly, T_{M2} can be considered to be a signed file 'valid to' time in epoch time, whereby an export must not be accepted if epoch time is after this time. T_{M1}= T_{M2}=4 bytes.

Once the token information and Session ID S_i has been forwarded to the Sender Entity local parameters T_{M1}, T_{M2} are re-evaluated in consideration of the CRA 7 time limits. The Sender Entity 6 then proceeds to create a File Token F_t which is used to create an Export Header comprising A_t, L_t, and F_t. The Nonce is randomly generated per file to be sent. The purpose of the Nonce N generated by the Sender Entity is that it provides entropy in L_t thereby allowing identical files authorised by the same Authorisation Token to have different Export Headers, and thereby allow them to be uniquely identified.

For the avoidance of doubt, the following parameters must be fed into the hash function as a single bytestream so as to form the File Token F_t:

A. The Local Token L_t;

B. The bytestream of the filename (with no null termination) J;

C. S_i; and

D. The payload X

The output from the hash calculation is F_t=#(X, L_t, J, S_i). This is used to create the Export Header as shown in Figure 5.

The first 96 bytes are the Authorisation Token A_t as obtained from the CRA the next 32 bytes are the Local Header L_t (assertions and other values made by the Sender) padded to 32 bytes. The last 32 bytes is the File Token F_f.

The filename parameter is used to create the hash, but it does not appear in the header.

As can be seen in Figure 5, null padding is provided in the header (which is an artefact of making the hashing functions more efficient). The export header is prepended to the payload X and then forwarded onwards to the predetermined Boundary Control Device by the Sender Entity.

At the Boundary Control Device the equivalent Session ID S_i is determined using HMAC (K_G, A_t) as will now be explained.

For convenience, the file to be exported is prepended with three tokens as per that shown in Figure 5. The first part is the Authorisation Token A_t of 96 bytes. Using A_t as the message for the HMAC function and Boundary Control Devices' K_G' as the key provides the Boundary Control Device's Session ID S_i'.

The file name is not present in the header, but can be determined using the shared identity information at the egress file transfer gateway.

At the Boundary Control Device there is then calculated the BCD File Token

F_t'=#(X, L_t, J, S_i'). This is the same calculation as that carried out by the Sender Entity, which is enabled due to the shared knowledge of the secret Permanent identity ID (being mindful however that the Sender Entity 6 never receives ID, but instead receives S_i in the Release Token). It is therefore once again reiterated that the Sender entity 6 does not have access to the Permanent ID K_G or K_G' (where K_G=K_G' if the correct Boundary Control Device is used). Both S_i'' and H' generated at the Boundary Control Device 3 have a size of 32 bytes.

To operate correctly, the Boundary Control Device 3 must agree on a time reference with the CRA 7 and Sender entity 6. Further, the Boundary Control Device is configured to only accept or egress file formats it has been configured to process.

It has been described that the passage of the payload through the Boundary Control Device is only permitted when the File Token generated by the Sender entity is identical to the File Token generated at the predetermined Boundary Control Device 3 i.e. F_t=F_t', however other predetermined conditional criteria must also be met. For example the following must also be true to enable transfer through the Boundary Control Device:

1. The file type declared must match the file format criteria specified at the Boundary Control Device;
2. The time of testing T_t in the Boundary Control Device must satisfy the following:
    a. $T_{M1} \leq T_t \leq T_{M2}$;
    b. $T_{S1} \leq T_t \leq T_{S2}$;
3. The file size must satisfy $S_{determined} \leq S$ or S=0;

4. The version parameter criteria must satisfy: $V_{gateway}=V$; and

Only if the Export Header of the payload contains an unchanged Authorisation Token A_t, with valid values of size, type, version, and validity times can the comparator ephemeral identity S_i' generated by the Boundary Control Device 3 be the same as S_i generated by the CRA 7. Also, the F_t' calculated by the Boundary Control Device 3 can only be the same as generated by the Sender Entity if the same Authorisation and Local tokens, and session ID are used as for the generation of F_t.

In an alternative example of the invention, a user wishes to export a Word Document.

The Sender entity 6 has previously asked the CRA 7 for a Release Token to perform this task which is in line with CRA 7 authorisation requirements. In possession of a valid Release Token, comprising an ephemeral identity, the Sender entity 6 creates an export header with the assertion that "This is a releasable Word Document" and the Sender entity 6 creates an export payload by prepending the export Header to the document – this header is derived from the Authorisation Token, ephemeral identity and local parameters.

The export header is formatted from three headers A_t, L_t and F_t. A_t is the allowed top-level properties which must be true and as specified by the CRA 7. H3 comprises the local assertions i.e. the local assertions made by the Sender entity 6 and relating to the payload properties. F_t is the output of the hash function which can also be determined at the Boundary Control Device 3 using the secret Permanent Identity Information (ID) (assuming the correct Boundary Control Device undertakes the calculation of the F_t').

This new export file (export header and payload) is then passed to the Boundary Control Device 3 e.g. gateway. The Boundary Control Device 3 makes a series of predetermined checks e.g. If F_t=F_t' then the criteria checks commence. These are checks for constraints that are assurable at the Boundary Control Device 3– i.e. the gateway makes an independent assessment of parameter checks assigned to it during factory setting e.g. file size or file type. If and only if all checks are valid will the payload X be released.

For the avoidance of doubt, this conditional criteria comparison and test at the Boundary Control Device 3 means that the Boundary Control Device independently verifies the truth of the suitability of file payload transfer across the network domain boundary.

In the simplest system (A_T and F_t) there is only one egress header per file where the actual physical Boundary Control Device used to egress must be picked by the Sender Entity 6 at the time of requesting the Authorisation Token so as to enable the use of the correct secret identifier information, K.

It is workable to add fields to the various tokens to provide further required criteria that is desired by the user. For example, the Classification of a file cannot be determined by the Boundary Control Device since there is unlikely to be mechanism to determine Classification based on payload at the Boundary Control Device 3.

For example, to enable document classification authorisation the classifications are transformed into a numerical representation to enable the Boundary Control Device to check it. Several schemes are available to the user and no such scheme has an indefinite lifetime.

One such scheme creates a new Authorisation Token parameter called "Classification" which can be used to describe the maximum classification of document that is allowed to egress the Boundary Control Device. A typical scheme would be the classifications (OFFICIAL, CONFIDENTIAL, SECRET, TOP SECRET). Similarly, for the Local Token this also has a defined parameter called Classification with the same permitted values which is the value of the Classification that is asserted by the Sender.

These permitted values are then mapped into numerical values for each header. One such scheme would be

- OFFICIAL – 100
- CONFIDENTIAL – 200
- SECRET – 300
- TOP SECRET - 400

To implement this the Boundary Control Devices would have to be instructed to compare the pair of encoded values in the Export Header against a specific logical operation. In this case A_t:Classification >= L_t:Classification.

Other characteristics features of protective marking schemes can be similarly handled within the Boundary Control Device using different logical operators to compare the mapped values in the various Tokens that make up the Export Header.

Alternatively, to more easily and directly determine the intended gateway from the header, as an example there be used 6 bytes of header to allow identification of the Boundary Control Device 3 directly. The 6-bytes identify the MAC address of the Boundary Control Device 3, which in full is six bytes (48 bits).

To map this into a name space such as would be required by DNS then the hex encoding the byte values suffice. For example, if the MAC address were in a hex representation "14-B3-1F-12-CB-E7" then the query to DNS will be "gw14B31F12CBE7.domain.tld" which resolves the IP address of the gateway based on the content of the Export Header using locally determined conventions. Whilst the gateway does not undertake any comparisons with this field, it does use the field as part of the normal authorised header in the hash calculation it undertakes as part of the assurance of authorisation process.

Various modifications to the principles described above would suggest themselves to the skilled person. For example, in an alternative embodiment of the invention, the authorisation token A_t does not incorporate the authorised file parameters in the form of authorisation values e.g. there is no provision of file size or other criteria checks associated with the file parameters at the CRA 7 and as such A_t=<entropy element> which provides a unique value per token element required. Session ID is created by taking a one-way function of the permanent Boundary Control Device ID (which is known by the CRA 7) and the Authorisation Token. A Release Token is subsequently composed of the Authorisation Token A_t and the Session ID S_i and is sent to the Sender Entity 6. The Sender Entity then calculates the File Token F_t= #(X, J, S_i) as previously described and then combines this with the Authorisation Token A_t to provide the Export Header, which in this instance E= A_t || F_t as there is no Local Token in this particular embodiment. The Export Header is prepended to the payload X which is to be transferred across the Boundary Control Device 3. In this most basic embodiment of the invention there is merely undertaken the most basic

verification checks at the Boundary Control Device and there are no checks performed against properties asserted by the Central Service. This embodiment clearly provides less CRA 7 control of the files or payloads to pass across the Boundary Control Device 3. It does, however, ensure the signed export file having payload X is transferred by a predetermined Boundary Control Device since the Boundary Control Device can determine an ephemeral key derived from its K_g and can check for the criteria $F_t=F_t'$.

The function to generate the ephemeral key may not comprise HMAC, but may comprise an alternative hash function e.g. a simple Hash.

An alternative implementation of the scheme as shown in Figure 6, is that the role of the Sender 6 described above is split into a Signer entity 13 and a Sender entity 6, where the Signer entity 13 is responsible for interactions with the CRA 7 and the creation of the Export Header, and the Sender entity 6 is responsible for requesting an Export Header for a payload.

In another embodiment where the payload is essentially unnamed, such as a network packet, then the File Token may be constructed using no Filename Value J

$F_t = \#(X, L_t, S_i)$

Alternatively a fixed string J such as “PACKET” could be used for such applications.

In another embodiment the values in the headers can be used individually as parameters to the hash functions. Similarly, some parts of the header may be permitted to be zeroed before use. These approaches allow predetermined parts of the header to be writable by intermediate systems between the Sender and

the Boundary Control System for administrative purposes not related to the Export Control Scheme, and still allow the Export Control Scheme to enforce the required security outcomes.

At the Sender entity it is envisaged that other suitable release controls known to the person skilled in the art exist which must also be satisfied prior to signing of the payload and the subsequent payload transfer.

It is noted that the scheme does not specify how identification, authentication and authorisation between the various non-gateway parties are performed since this is believed to extend outside the scope of this invention. However, for the purpose of the invention described herein, it is assumed that this has been completed satisfactorily prior to any payload transfer request.

All parameters may be of a different size than indicated in the embodiments described herein and the above-mentioned parameter sizes are for example only and are not to be considered a limiting feature of the invention.

Alternatively, in use the system may be an integral element within a computational device.

Alternatively, the system may be a modular component of a network infrastructure to ensure self-authorising and reliably assured transfer of payloads between network nodes.

In a further embodiment of the invention the payload property is merely the time of request when as a minimum the system supplies authorisation for use for a limited period.

In an alternative embodiment of the invention, the File Token also comprises the Authorisation Token $F_t=g(X, A_t, L_t, S_i)$, for example $F_t=\#(X, A_t, L_t,$

S_i). Therefore, the assurance scheme is still valid where additional information is incorporated in the calculation, although this will likely increase the processing effort without any significant advantage being provided.

Commonly, in the above-mentioned embodiments of the invention first network 8 is a trusted network and the second network 9 is a lesser trusted network, however in a yet further alternative embodiment of the invention the fpayload may be an import payload in the form of an import payload/file and as such the first network may be the lesser trusted network and the second network may be a trusted network.

The system beneficially i. removes the need for re-configuration of payload transfer criteria at the Boundary Control Device, thereby eliminating the need to patch software located at the Boundary Control Device, ii. removes the need to locally manage the Boundary Control Device and therefore offers the ability to use a sealed-for-life gateway that is maintained at factory settings. All the above-mentioned benefits minimise the attack surface associated with the Boundary Control Device at a local level. Advantageously, the number of assurable assertions at the Boundary Control Device 3 can be made small, allowing for a relatively invariant Boundary Control Device capable of providing a stronger security function compared to existing security devices, since decisions are guaranteed to be specified and enforced at the CRA 7. This security benefit is achieved whilst offering an agile device and method which provides specification of permitted parameters remotely from the gateway by an authoriser entity (the CRA 7), removing the need for the Boundary Control Device 3 to have any knowledge of the decision making process concerning the

preferred payload transfer parameters.

The above described embodiments of the invention all enable the following benefits:

- Senders and Gateways can be highly scalable, highly available;
- CRA (with a sensible Ticket Book validity period) does not need to be highly available;
- Keys highly sensitive stored very securely; and
- Session IDs moderately sensitive – expire regularly so no long-term risk.
- Optimisations for efficiency in real world applications are possible by careful choice of Export Header contents.

CLAIMS

1. A payload assurance system for a payload X having a header H which is to be transferred across a network boundary via at least one predetermined boundary control device, the system comprising 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 provide an electronic authorisation token for authorising properties of the payload to be transferred, the electronic authorisation token comprising at least one entropy element for ensuring that multiple electronic authorisation tokens authorising the same payload properties are unique.
2. A payload assurance system according to claim 1 comprising multiple separate and distinct electronic entities, comprising of at least one Authoriser entity, at least one Sender entity and at the least one Boundary Control Device.
3. A payload assurance system according to claim 2, wherein the Authoriser entity is configured to create an ephemeral identity for a predetermined Boundary Control Device using the electronic authorisation token and permanent identity information associated with the predetermined Boundary Control Device.
4. A payload assurance system according to claim 3, wherein the permanent identity information for each Boundary Control Device in the system is stored at the Authoriser entity.

5. A payload assurance system according to claim 3 or claim 4, wherein the at least one Authoriser entity is configured to transfer the ephemeral identity to the Sender entity upon request.
6. A payload assurance system according to claim 5 wherein the Sender entity is configured to create an export or import header in dependence upon the ephemeral identity to be forwarded to the Boundary Control Device.
7. A payload assurance system according to any of claims 2 to 4, wherein there is further provided at least one Signer entity, wherein the Signer entity is located communicatively intermediate the at least one Authoriser entity and the at least one Sender entity, so as to prevent the at least one Sender entity from communicating directly with the Authoriser entity.
8. A payload assurance system according to claim 7 when dependent on claim 3 or claim 4, wherein the Authoriser entity is configured to transfer the ephemeral identity to the Signer entity upon request.
9. A payload assurance system according to claim 8 wherein the Signer entity is configured to create an export or import header in dependence upon the ephemeral identity and to subsequently forward it to the Sender entity.
10. A payload assurance system according to claim 6 or claim 9, wherein the Sender entity is configured to append the export or import header to the payload to form an export Payload and to subsequently transfer the export payload to the predetermined Boundary Control Device.

11. A payload assurance system according to claim 10, wherein the export or import payload header further comprises a local token defining local properties of the payload to be transferred.

12. A payload assurance system according to any of claims 3 to 11, wherein the Authoriser entity is configured to provide an ephemeral identity of the Boundary Control Device in dependence upon the electronic authorisation token and the permanent identity information of the predetermined boundary control device by implementing a one-way mathematical function.

13. A payload assurance system according to claim 12, wherein the one-way mathematical function comprises a HMAC, having an associated secret key.

14. A payload assurance system according to claim 13, wherein the secret key comprises the permanent identity information for the predetermined Boundary Control Device.

15. A payload assurance system according to any of claims 2 to 14, wherein the at least one Sender entity is the sole electronic entity in communication with the at least one Boundary Control Device.

16. A payload assurance system according to any of claims 2 to 15, wherein the Boundary Control device comprises a comparator, the comparator being configured to, upon receipt of the payload to be exported or imported, directly or indirectly identify the authorisation token in the export or import payload header and to create a comparator ephemeral identity in dependence upon the authorisation token and its locally stored permanent identity information.

17. A payload assurance device according to claim 16, the comparator being configured to directly or indirectly compare the ephemeral identity generated at the at least one Authoriser entity with the comparator ephemeral identity generated at the at least one Boundary Control Device so as to determine whether they are the same.

18. A payload assurance device according to claim 17, the comparator being further configured to compare other control criteria contained in the export or import payload header to ensure they are within predefined limits.

19. A payload assurance system according to claim 18, the comparator being configured to determine a positive boundary control outcome in the case that

i. the ephemeral identity generated is the same as the comparator ephemeral identity; and

ii. the other export or import header control criteria are within the predefined limits.

20. A payload assurance system according to claim 19, wherein the Boundary Control Device is configured to transfer a payload X having associated header H through the Boundary Control Device and across a network/domain boundary in the case that a positive boundary control outcome has been met.

21. A payload assurance system according to claim 19, wherein the Boundary control device is configured to prohibit passage of the payload X hav-

ing associated Header H across the network/domain boundary and/or enable the payload X to be dropped in the case that a positive boundary control outcome has not been met.

22. A payload assurance system according to any preceding claim, comprising a random number generator or pseudo random number generator for providing the entropy element of the electronic authorisation token.

23. A payload assurance system according to any preceding claim, wherein the electronic authorisation token is publicly known.

24. An export control system for transferring an export payload X having a Header H across the Network Boundary comprising the payload assurance system according to any preceding claim.

25. A method of assuring a payload for transfer across a network boundary via a Boundary Control Device using a system comprising 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 processor, the method comprising providing an electronic authorisation token configured to authorise the payload to be transferred, the electronic authorisation token comprising at least one element relating to properties of the payload and at least one entropy element for ensuring that multiple electronic authorisation tokens authorising the same payload properties are unique.

26. A method according to claim 25, the system further comprising at least one Authoriser entity and at least one Sender entity configured communicatively intermediate the Authoriser entity and Boundary Control Device,

the method further comprising creating an ephemeral identity for a predetermined Boundary Control Device using the electronic authorisation token and permanent identity information associated with the predetermined Boundary Control Device.

27. A method according to claim 26 further comprising providing the ephemeral identity of a predetermined Boundary Control Device in dependence upon the electronic authorisation token and permanent identity information of the predetermined boundary control device by implementing a one-way mathematical function.

28. A method according to claim 27, wherein the one-way mathematical function comprises a HMAC, having an associated secret key.

29. A method according to claim 28 when dependent on any of claims 26 to 27, wherein the secret key comprises the permanent identity information for the predetermined Boundary Control Device.

30. A method according to any of claims 26 to 29, comprising storing the permanent identity information for each Boundary Control Device in the system at the Authoriser entity.

31. A method according to claim 26 or 29, comprising prohibiting the permanent identity information from being accessed by the Sender entity.

32. A method according to any of claims 26 to 31, wherein the Authoriser entity transfers the ephemeral identity to the Sender entity upon request, the Sender entity subsequently creating an export or import header in dependence upon the ephemeral identity.

33. A method according to any of claims 26 to 31, wherein the system further comprises a Signer entity and the Authoriser entity transfers the ephemeral identity to the Signer entity upon request, the Signer entity subsequently creating an export or import header in dependence upon the ephemeral identity and subsequently forwarding it to the Sender entity.

34. A method according to claim 32 or 33, further comprising providing the ephemeral identity of the predetermined Boundary Control Device in the export or import header.

35. A method according to claim 34, comprising appending the export or import header to the payload at the Sender entity so as to create an export or import payload having Header H respectively and subsequently forwarding the export or import payload having Header H to the predetermined Boundary Control Device.

36. A method according to any of claims 32 to 35, comprising providing local properties of the payload to be transferred in the export or import header.

37. A method according to any of 32 to 36, wherein upon receipt of the export or import payload having Header H at the Boundary Control Device the method further comprising identifying the authorisation token in the export or import payload header; and creating a comparator ephemeral identity in dependence upon the authorisation token and the permanent identity information locally stored at the Boundary Control device.

38. A method according to claim 37, further comprising directly or indirectly comparing the ephemeral identity generated at the Authoriser entity with

the comparator ephemeral identity generated at the Boundary Control Device to determine whether they are identical.

39. A method according to claim 38, the comparator being further configured to compare other control criteria contained in the export or import header to ensure they are within predefined limits.

40. A method according to claim 39, comprising determining a positive boundary control outcome in the case that

i. the ephemeral identity generated at the Authoriser entity is the same as the comparator ephemeral identity generated at the Boundary Control Device; and

ii. the other export or import header control criteria are within the predefined limits.

41. A method according to claim 40, comprising transferring the payload X having associated Header H through the Boundary Control Device and across a network/domain boundary when the positive boundary control outcome has been met.

42. A method according to claim 40, comprising prohibiting passage of the Payload X having associated Header H and/or enables dropping of the Payload X in the case that a positive boundary control outcome has not been met.

43. A method according to any of claims 25 to 42 comprising randomly or pseudo randomly generating a value to provide the entropy element of the electronic authorisation token.

44. A method according to any of claims 24 to 42, comprising determining the electronic authorisation token lifetime to be $T_{S1} \leq T_t \leq T_{S2}$ such that the authorisation is determined to be valid for the electronic authorisation token lifetime.

45. A method according to any of claims 25 to 43, comprising determining an export or import time period as $T_{M1} \leq T_t \leq T_{M2}$ such that the export or import of the payload X is only permitted when the respective export or import period is satisfied.

46. A method according to any of claims 26 to 45, comprising calibrating and/or agreeing a time reference between the Authoriser entity and the at least one predetermined Boundary Control Device.

47. A computational device comprising a system for assuring a payload for transfer from a lesser trusted network to a trusted network (or vice versa) according to any of claims 1 to 24.

48. A network comprising a system for assuring a payload for transfer from a lesser trusted network to a trusted network (or vice versa) according to any of claims 1 to 24.