

netic or optical drive or diskette) and operated by the CPU in the memory 404 of the computer. As such, the border guard module or device 405 (including associated data structures and methods employed within the encoder) of the present invention can be stored on a computer readable medium or carrier, e.g., RAM memory, magnetic or optical drive or diskette and the like.

While the foregoing is directed to embodiments of the present invention, other and further embodiments of the invention may be devised without departing from the basic scope thereof, and the scope thereof is determined by the claims that follow.

The invention claimed is:

1. A method for defining rules and enforcing rules of transitioning a digital content between two security domains having different security requirements, the method comprising:
  - establishing a first security domain for receiving, from a digital content source, a transport stream comprising a digital content;
  - establishing a second security domain associated with devices for storage of the digital content at a receiver device, wherein the second security domain is established at the border of the first security domain and the second security domain;
  - wherein the digital content source can cause the digital content to be pre-positioned on the receiver device while the digital content remains in the first security domain, and the digital content source also can cause the digital content to be transmitted from the first security domain to the second security domain; and
  - if the digital content source causes the digital content to be pre-positioned on the receiver device while the digital content remains in the first security domain:
    - receiving and storing the digital content on the receiver device with transport security associated with the first security domain kept intact and with encryption associated with the first security domain kept intact;
    - otherwise, if the digital content source causes the digital content to be transmitted from the first security domain to the second security domain:
      - performing authorization for conditional access of transport stream from the first security domain;
      - providing a session ID for authorizing both a program and associated digital rights management (DRM) rules received with the digital content in the first security domain, and authenticating each session request received from a particular device in the second security domain for usage of the digital content;
      - selecting at least one rule from the DRM rules to be transmitted with the digital content;
      - transmitting the at least one rule with the digital content from the first security domain to the second security domain;
      - translating a first protection in the first security domain of the digital content and the at least one rule attached to the digital content to a second protection in the second security domain of the digital content and the at least one rule for secure delivery and locking the usage of the digital content to the particular device in the second security domain;
      - continuously enforcing the at least one rule during usage of the digital content in the second security domain; and
      - maintaining control over the usage of the digital content in the second security domain.
2. The method of claim 1, wherein said first security domain is a transport domain.

3. The method of claim 2, wherein said second security domain is a persistent security domain.

4. The method of claim 1, wherein said translating is performed by a border guard in the receiver device, wherein the border guard further comprises a security device, further wherein the security device comprises an application specific integrated circuit (ASIC).

5. The method of claim 4, wherein said border guard enforces said at least one rule associated with how an associated content of the digital content is moved between said first and second domains.

6. The method of claim 5, wherein said at least one rule is specified by a source of said associated content and is enforced by said border guard.

7. The method of claim 5, further comprising:
 

- employing a portable renewable security card, where said border guard operates cooperatively with said portable renewable security card for enforcing said at least one rule for transition between said first and second security domains.

8. A non-transitory computer-readable medium having stored thereon a plurality of instructions, the plurality of instructions including instructions which, when executed by a processor, cause the processor to perform the steps of a method for defining rules and enforcing rules of transitioning a digital content between two security domains having different security requirements, comprising:

establishing a first security domain for receiving, from a digital content source, a transport stream comprising digital content;

establishing a second security domain associated with devices for storage of the digital content at a receiver device, wherein the second security domain is established at the border of the first security domain;

wherein the digital content source can cause the digital content to be pre-positioned on the receiver device while the digital content remains in the first security domain, and the digital content source also can cause the digital content to be transmitted from the first security domain to the second security domain; and

if the digital content source causes the digital content to be pre-positioned on the receiver device while the digital content remains in the first security domain:

receiving and storing the digital content on the receiver device with transport security associated with the first security domain kept intact and with encryption associated with the first security domain kept intact;

otherwise, if the digital content source causes the digital content to be transmitted from the first security domain to the second security domain:

performing authorization for conditional access of transport stream from the first security domain;

providing a session ID for authorizing both a program and associated digital rights management (DRM) rules received with the digital content in the first security domain, and authenticating each session request received from a particular device in the second security domain for usage of the digital content;

selecting at least one rule from the DRM rules to be transmitted with the digital content;

transmitting the at least one rule with the digital content from the first security domain to the second security domain;

translating a first protection in the first security domain of the digital content and the at least one rule attached to the digital content to a second protection in the second security domain of the digital content and the