

output port, a user input device (such as a keyboard, a keypad, a mouse, and the like), or a microphone for capturing speech commands).

It should be understood that the security device **305** can be implemented as a physical device or subsystem that is coupled to the CPU **302** through a communication channel. Alternatively, the security device **305** can be represented by one or more software applications (or even a combination of software and hardware, e.g., using application specific integrated circuits (ASIC)), where the software is loaded from a storage medium (e.g., a magnetic or optical drive or diskette) and operated by the CPU in the memory **304** of the computer. As such, the security device **305** (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 processing a system time reference, said method comprising:

receiving, by a subscriber receiving device, a system time reference and a time sequence number from a content provider;

determining whether said system time reference received from said content provider is legitimate, wherein said determining uses said received time sequence number to determine whether said system time reference is legitimate; and

synchronizing a local clock reference of said subscriber receiving device to said system time reference if said system time reference is determined to be legitimate.

**2.** The method of claim **1**, wherein said system time reference is received in a secure system time message.

**3.** The method of claim **2**, wherein said secure system time message is a broadcasted message.

**4.** The method of claim **2**, wherein said secure system time message is an encrypted or authenticated message.

**5.** The method of claim **1**, wherein said determining comprises:

determining said system time reference to be legitimate if:  
1) said received time sequence number is equal to a locally stored time sequence number, and 2) said system time reference is greater than said local clock reference.

**6.** The method of claim **1**, wherein said determining comprises:

determining said system time reference to be legitimate if:  
1) said received time sequence number is different from a locally stored time sequence number by a predefined difference value, and 2) said system time reference is greater than said local clock reference.

**7.** The method of claim **1**, wherein said determining comprises:

determining said system time reference to be legitimate if:  
1) said received time sequence number is different from a locally stored time sequence number by a predefined difference value, and 2) said system time reference is less than or equal to said local clock reference.

**8.** The method of claim **1**, further comprising:  
using said local clock reference to enforce a time based usage rule of a locally stored multimedia content.

**9.** 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 steps for processing a system time reference, the steps comprising:

receiving a system time reference; receiving a time sequence number; determining whether said system time reference is legitimate, wherein said determining uses said received time sequence number to determine whether said system time reference is legitimate; and synchronizing a local clock reference to said system time reference if said system time reference is determined to be legitimate.

**10.** The non-transitory computer-readable medium of claim **9**, wherein said system time reference is received in a secure system time message.

**11.** The non-transitory computer-readable medium of claim **10**, wherein said secure system time message is a broadcasted message.

**12.** The non-transitory computer-readable medium of claim **10**, wherein said secure system time message is an encrypted or authenticated message.

**13.** The non-transitory computer-readable medium of claim **9**, wherein said determining comprises:

determining said system time reference to be legitimate if:  
1) said received time sequence number is equal to a locally stored time sequence number, and 2) said system time reference is greater than said local clock reference; or

determining said system time reference to be legitimate if:  
1) said received time sequence number is different from a locally stored time sequence number by a predefined difference value, and 2) said system time reference is greater than said local clock reference; or

determining said system time reference to be legitimate if:  
1) said received time sequence number is different from a locally stored time sequence number by a predefined difference value, and 2) said system time reference is less than or equal to said local clock reference.

**14.** The non-transitory computer-readable medium of claim **9**, the steps further comprising:

using said local clock reference to enforce a time based usage rule of a locally stored multimedia content.

**15.** An apparatus for processing a system time reference, said apparatus comprising:

a subscriber receiving device for receiving a system time reference and a time sequence number from a content provider; and

a processor of said subscriber receiving device, the processor being configured to:

determine whether said system time reference received from said content provider is legitimate, wherein said determining uses said received time sequence number to determine whether said system time reference is legitimate, and

synchronize a local clock reference to said system time reference if said system time reference is determined to be legitimate.

**16.** The apparatus of claim **15**, where said subscriber receiving device is at least one of a set top box and a receiver.