PATROLL Winning Submission

U.S. Patent 8,291,236

U.S. Patent 8,291,236 ("*Videolabs*" or the "patent-at-issue") was filed on December 7, 2004 and claims priority on the same date. Claim 1 of the patent-at-issue is generally directed to a method of managing the display of a content. The method involves obtaining a representation of the content from a primary conditional access server, which encrypts the content and employs a specific set of cryptographic keys to protect it within a designated security domain. Upon a user's request, the content is presented via a secondary conditional access server linked to the primary one and is authorized via a client-server relationship between the secondary and primary servers respectively. The secondary server also utilizes a distinct set of cryptographic keys to ensure the content remains protected within a different security domain during its presentation. Furthermore, the primary server verifies the secondary server as one of its client devices through an initial authentication process, employing a primary root of trust. The secondary server then authenticates its client devices using a separate authentication process and employing a secondary root of trust distinct from the primary. Additionally, the secondary server is designed to substitute the security domain of the primary server with its own for its client devices under its unique root of trust.

The primary reference, U.S. Pat. App. 2005/0105732 ("*ARRIS*"), was filed on November 12, 2004, and claims an earliest priority date on November 17, 2003. The patent application describes a content delivery system capable of distributing pre-encrypted content to a primary subscriber terminal. The system is composed of an offline encryption system, a caching system, a first conditional access system, a second conditional access system, and a first encryption renewal system linked to the first conditional access system. The offline encryption system creates pre-encrypted content utilizing a control word, while the caching system stores and transmits this pre-encrypted content to the primary subscriber terminal. The first conditional access system permits multiple subscriber terminals to decrypt the pre-encrypted content, while the second conditional access system facilitates decryption specifically for the primary subscriber terminal. The first encryption renewal system, associated with the first conditional access system, authorizes the second conditional access system to enable decryption for the primary subscriber terminal.

The secondary reference, U.S. Pat. App. 2005/0144478 ("*Toshiba*"), was filed on October 4, 2004, and claims an earliest priority date on December 25, 2003. The patent application describes a content delivery system with an enhanced security feature, preventing the reproduction of content whose valid usage period has expired. The system includes an initial encryption means for generating a content key to encrypt selected content and decrypting said encrypted content. In addition, the system also has a secondary encryption to produce a primary encryption key, encrypting the content key to form an encrypted content key. The system also utilizes a primary delivery means to transmit the encrypted content and content key. Further, the system also has a secondary delivery means to generate a decryption key and an encryption key upon receiving a reproduction request for specific content, transmitting both keys via the network. The system then decrypts the encrypted content key using the delivered decryption key, while secondary decryption decrypts the encrypted content using the decrypted content key.

A sample claim chart comparing claim 1 of *Videolabs* to *ARRIS* and *Toshiba* is provided below.

US8291236 ("*Videolabs*")	**A. US20050105732** (*"ARRIS"*) **B. US20050144478** (*"Toshiba"*)
1.pre. A method to **control a presentation of content**, the method comprising:	**A. US20050105732** "1. A **content delivery system for delivering pre-encrypted content** to a first subscriber terminal, said system comprising: . . ." *ARRIS* at claim 1 "Systems and **methods for delivering pre-encrypted content to one or more subscriber terminals whose access to the pre-encrypted content is controlled** by two or more conditional access (CA) systems are described herein." *ARRIS* at par. 0014 **B. US20050144478** "1. A **content delivery system** comprising: . . ." *Toshiba* at claim 1
1.a. **receiving a representation of content from a first conditional access server** which **provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in a first security domain**; and	**A. US20050105732** "1. A content delivery system for delivering pre-encrypted content to a first subscriber terminal, said system comprising: **an off line encryption system configured to generate said pre-encrypted content using a control word**; a caching system configured to store said pre-encrypted content and **transmit said pre-encrypted content to said first subscriber terminal**; **a first conditional access system configured** to allow a number of subscriber terminals **to decrypt said pre-encrypted content**; . . . . " *ARRIS* at claim 1 "Among other components, the content delivery system (100) comprises a content generation system (100) for generating clear content, an off line encryption system (OLES) (101) for pre-encrypting the content, a video on-demand (VOD) system (102) for storing the pre-encrypted content and for distributing the pre-encrypted content to the STB (103) on an on-demand basis, **a conditional access system (CAS)** (121) **for controlling one or more keys granting access to pre-encrypted content**, ..." *ARRIS* at par. 0018 "FIG. 4 shows a first content delivery system (150) and a second content delivery system (151) configured to share the same pre-encrypted content. The **first content delivery system**

(cont.) 1.a. **receiving a representation of content from a first conditional access server** which **provides the content in an encrypted form and uses a first set of cryptographic keys to protect the content from unauthorized access in a first security domain**; and	(150) **includes the content generation system** (100) **that generates the content and the OLES** (101) **that pre-encrypts the content**. The first content delivery system (150) also includes a first ERS (131-1) configured to control the participation of a number of CA systems (121-4) in the first content delivery system (150). The first content delivery system (150) may also include, but is not limited to, a VOD system (102-1) and a number of STBs (103-4).” *ARRIS* at par. 0046 **B. US20050144478** “1. A content delivery system comprising: **first encryption means for generating a content key for encrypting selected content to generate encrypted content**, and decrypting the encrypted content; second encryption means for **generating a first encryption key for encrypting the content key to generate an encrypted content key**; . . . .” *Toshiba* at claim 1 “3. A content receiving/storing apparatus that **receives and stores encrypted content via a network**, wherein each time the encrypted content is to be decrypted, **request information for requesting an encrypted content key for decrypting the encrypted content is transmitted**, and **the encrypted content key corresponding to the request information is received and used for the decryption of the encrypted content**.” *Toshiba* at claim 3
1.b. **presenting the content**, at a user's request, **through a second conditional access server which is coupled to the first conditional access server**;	**A. US20050105732** “A caching server stores the pre-encrypted content and **transmits the pre-encrypted content to the STB**. An **encryption renewal system associated with a first conditional access system authorizes a second conditional access system to allow one or more subscriber terminals to decrypt the pre-encrypted content**.” *ARRIS* at par. 0014 “1. A content delivery system for **delivering pre-encrypted content to a first subscriber terminal**, said system comprising: . . . **a second conditional access system configured to allow said first subscriber terminal to decrypt said pre-encrypted content**; and . . . .” *ARRIS* at claim 1

(cont.) 1.b. **presenting the content**, at a user's request, **through a second conditional access server which is coupled to the first conditional access server**;	"An **STB** (103) **will be used in the following examples as an exemplary subscriber terminal**." *ARRIS* at par. 0018 "**Any STB** (103) **associated with CAS** (121-1) **may then request pre-encrypted content** from the VOD system (102). For example, STB (103-1) may request pre-encrypted content from the VOD system (102). If CAS (121-1) authorizes STB (103-1) to receive the requested pre-encrypted content, CAS (121-1) transmits EMM to STB, (103-1)." *ARRIS* at par. 0041 **B. US20050144478** "1. A content delivery system comprising: . . . **first delivery means for delivering via a network the encrypted content that is encrypted by the first encryption means and the encrypted content key that is encrypted by the second encryption means**; . . . ." *Toshiba* at claim 1 "The content delivery system according to the embodiment comprises: a content delivery server 2 that is connected to a network 5 such as a WAN (Wide Area Network) or the Internet; **a content database** 1 and a license server 4, **which are connected to the content delivery server** 2, a license database 3 that is connected to the license server 4; **a local server** 6 **that is connectable to the content delivery server** 2 via the network 5; a storage device 7 that is connected to the local server 6, and **a user terminal** 9a **and a user terminal** 9b, **which are connectable to the local server** (content receiving/storing apparatus) 6 via a LAN (Local Area Network) 8." *Toshiba* at par. 0031 "The content database stores a plurality of **contents for delivery to a plurality of user terminals** such as the user terminals 9a and 9b." *Toshiba* at par. 0033 "As is shown in FIG. 2, **the content delivery server** 2 **comprises a user authentication unit** 21 **that executes authentication with the user terminal** 9 a, 9 b; a database control unit 22 that executes a control such as transmission/reception of data with the content database 1; …" *Toshiba* at par. 0034 "As is shown in FIG. 5, **the user terminal** 9a, 9b **includes a communication control unit** 91 **that executes a series of processes including** at least user authentication and a **content delivery request**; a copy protect process unit 92 that executes

(cont.) 1.b. **presenting the content**, at a user's request, **through a second conditional access server which is coupled to the first conditional access server**;	a decryption process for copy-protected content that is delivered from the local server 6; a display unit 93 that reproduces or displays content that is requested; and an input unit 94 that inputs, e.g. a user ID and a password at a time of user authentication, and a request for content delivery." *Toshiba* at par. 0058
1.c. wherein the **presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively**;	**A. US20050105732** "A caching server stores the pre-encrypted content and **transmits the pre-encrypted content to the STB**. An **encryption renewal system associated with a first conditional access system authorizes a second conditional access system to allow one or more subscriber terminals to decrypt the pre-encrypted content**." *ARRIS* at par. 0014 "Once the clear content is pre-encrypted by the OLES (101), **the resulting pre-encrypted content and associated ER are delivered to the VOD system** (102) for storage. The VOD system (102) is configured to keep the pre-encrypted content and associated ER together. The **VOD system** (102) **may be any system or server configured to store and distribute pre-encrypted VOD content and/or any other type pre-encrypted content to one or more STBs** (103). The VOD system (102) is also referred to as a "VOD server," a "caching system," or a "caching server."" *ARRIS* at par. 0021 "FIG. 4 shows a first content delivery system (150) and a second content delivery system (151) configured to share the same pre-encrypted content. The first content delivery system (150) includes the content generation system (100) that generates the content and the OLES (101) that pre-encrypts the content. The **first content delivery system** (150) also **includes a first ERS** (131-1) configured to control the participation of a number of CA systems (121-4) in the first content delivery system (150). The first content delivery system (150) may also include, but is not limited to, a VOD system (102-1) and a number of STBs (103-4). **The second content delivery system** (151) **includes a second ERS** (131 2) **configured to control the participation of a number of CA systems** (121-5) in the second content delivery system (151)." *ARRIS* at par. 0046 "In some embodiments, **the first ERS** (131-1) **transmits the ER generated by the OLES** (101) **to the second ERS** (131-2) **so that the second content delivery system** (151) **may use its**

(cont.) 1.c. wherein the **presenting of the content is authorized through a client server relationship between the second and the first conditional access servers respectively**;	**own localized conditional access systems to secure access to the pre-encrypted content**." *ARRIS* at par. 0047 **B. US20050144478** "1. A content delivery system comprising: . . . **first delivery means for delivering via a network the encrypted content that is encrypted by the first encryption means and the encrypted content key that is encrypted by the second encryption means**; . . . ." *Toshiba* at claim 1 "**The delivery control unit** 23 **issues instruction information to the user authentication unit** 21, database control unit 22, key generation unit 24, encryption process unit 25, communication control unit 26 and license server 4 in order to execute a series processes: user authentication with the local server 6 (to be described later), **delivery of content information to the local server** 6, **confirmation and update of the user's content license (i.e. user's right to use content), encryption of content and a key for encrypting content (hereinafter referred to as "content key"), and delivery of key information**." *Toshiba* at par. 0037 "If the **delivery control unit** 23 **of content delivery server** 2 **receives the user authentication information from the local server** 6, the **delivery control unit** 23 **executes** user **authentication with use of the user authentication information and user database** 211 (step S605) and determines whether the authentication is successfully completed (Step S606). **If the** user **authentication is successful, the content delivery server** 2 **informs the local server** 6 **of the success in** user **authentication and establishes a session with the local server** 6." *Toshiba* at par. 0065
1.d. wherein **the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain**; and	**A. US20050105732** "FIG. 4 shows a first content delivery system (150) and **a second content delivery system** (151) **configured to share the same pre-encrypted content**. The first content delivery system (150) includes the content generation system (100) that generates the content and the OLES (101) that pre-encrypts the content. The first content delivery system (150) also includes a first ERS (131-1) configured to control the participation of a number of CA systems (121-4) in the first content delivery system (150). The first content delivery system (150) may also

(cont.) 1.d. wherein **the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain**; and	include, but is not limited to, a VOD system (102-1) and a number of STBs (103-4). **The second content delivery system** (151) **includes a second ERS** (131-2) **configured to control the participation of a number of CA systems** (121-5) **in the second content delivery system** (151). The second content delivery system (151) may also include, but is not limited to, a VOD system (102-2) and a number of STBs (103-5).” *ARRIS* at par. 0046 “2. The content delivery system of claim 1, wherein: . . . said **encryption renewal system uses said encryption record to generate an encrypted control word corresponding to said second conditional access system**, said **encrypted control word being an encrypted version of said control word used to pre-encrypt said content**.” *ARRIS* at claim 2 “8. The content delivery system of claim 2, wherein said **encryption renewal system transmits said encryption record and said encrypted control word corresponding to said second conditional access system to said caching system**, **said caching system comprising one or more storage units for storing said encryption record and said encrypted control word**.” *ARRIS* at claim 8 **B. US20050144478** “1. A content delivery system comprising: . . . **second delivery means** for generating, upon receiving a reproduction request for reproducing predetermined content, a first decryption key for decrypting the encrypted content key corresponding to the predetermined content, the reproduction request for which is received, and **a second encryption key for re-encrypting the decrypted content key that is decrypted by the first decryption key, and delivering the first decryption key and the second encryption key via the network**; . . . .” *Toshiba* at claim 1 “The decrypted content that is decrypted by the second decryption process unit 642 is input to the copy protect process unit 643, and a copy protect attribute of, e.g. “Never Copy', is added to the decrypted content. Thus, a copy prevention process for copy prevention on the user terminal side is executed, and the resultant decrypted content is sent to the user terminal 9a (step S508). If the user terminal 9a receives **the content that has been subjected to the copy prevention**

(cont.) 1.d. wherein **the second conditional access server uses a second set of cryptographic keys to protect the content from unauthorized access in presenting the content in a second security domain**; and	**process in the local server** 6, the copy protect process unit 92 executes a decryption process and outputs the decrypted content to the display unit 93." *Toshiba* at par. 0085
1.e. wherein **the first conditional access server authenticates the second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust** and **the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process** and	**A. US20050105732** "As shown in FIG. 3, **the ERS** (131) **may also exchange authorization data (CAS authorization data) with each authorized CA system** (121). In this manner, **the ERS** (131) **may control which CA system** (121) **participates in the content delivery system** (145). The authorization data may be exchanged via any communication protocol known in the art. For example, the communication protocol may be the SimulCrypt or authenticated Diffie Hellman protocol." *ARRIS* at par. 0044 "In some embodiments, **the first ERS** (131-1) **transmits the ER generated by the OLES** (101) **to the second ERS** (131-2) **so that the second content delivery system** (151) **may use its own localized conditional access systems to secure access to the pre-encrypted content**. As shown in FIG. 4, **an interface (certificate exchange) based on a certificate authentication protocol may be used to allow the first ERS** (131-1) **to securely transfer to the second ERS** (131-2) **the information needed to uncover or decrypt the ER**. The **second ERS** (131-2) **may then generate the control word used to pre-encrypt the content and use its own encryption scheme to generate ECWs, ECMs, and/or other forms of the control word**. The **certificate authentication protocol may be any protocol such as, but not limited to, the SimulCrypt protocol or the X.509 certificate exchange and verification protocol**." *ARRIS* at par. 0047 "10. The content delivery system of claim 1, wherein said **encryption renewal system authorizes said conditional access system to allow said first subscriber terminal to decrypt said pre-encrypted content by communicating with said second conditional access system using a key exchange protocol**." *ARRIS* at claim 10 "16. The content delivery system of claim 15, wherein said **first encryption renewal system transmits said encryption**

(cont.) 1.e. wherein **the first conditional access server authenticates the second conditional access server as one of client devices of the first conditional access server through a first authentication process using a first root of trust** and **the second conditional access server authenticates client devices of the second conditional access server through a second authentication process which is independent of the first authentication process** and	**data to said second encryption renewal system using a certificate authentication protocol**." *ARRIS* at claim 16 **B. US20050144478** "If the delivery control unit 62 of the local server 6 receives the content reproduction request, **the delivery control unit** 62 **requests user authentication information comprising a user ID and a password from the user terminal** 9 a. **Upon receiving the request for the user authentication information, the user terminal** 9 a **transmits via the input unit** 94 **the user authentication information comprising the user ID and password to the local server** 6. Receiving the user authentication information from the user terminal 9 a, the **delivery control unit** 62 **of local server** 6 **executes user authentication with use of the user authentication information and the user database** 632 (step S601) and determines whether the authentication is successfully completed (step S602). If the user authentication is successful, **the delivery control unit** 62 **transmits the user authentication information to the content delivery server** 2 **via the first communication control unit** 61 **and network** 5, **and then establishes a session with the user terminal** 9 a (step S603). If the user authentication fails, the delivery control unit 62 informs the user terminal 9 a of the failure in user authentication and finishes the session (step S604)." *Toshiba* at par. 0064 "If the **delivery control unit** 23 **of content delivery server** 2 **receives the user authentication information from the local server** 6, the **delivery control unit** 23 **executes user authentication with use of the user authentication information and user database** 211 (step S605) and determines whether the authentication is successfully completed (Step S606). **If the user authentication is successful, the content delivery server** 2 **informs the local server** 6 **of the success in user authentication and establishes a session with the local server** 6." *Toshiba* at par. 0065
1.f. wherein **the second authentication process uses a second root of trust which is independent of and different than the first root of trust**, and wherein **the second conditional access server is**	**A. US20050105732** "27. The method of claim 19, wherein said step of using said **encryption renewal system to authorize said second conditional access system to allow said first subscriber terminal to decrypt said pre-encrypted content comprises using a key exchange protocol to communicate between**

configured to substitute the first security domain with the second security domain for the client devices under the second root of trust.	**said encryption renewal system and said second conditional access system**." ARRIS at claim 27 "In some embodiments, **the CA systems** (121) **periodically regenerate the ECMs**. These **regenerated ECMs are transmitted to the VOD system** (102) **to replace the previously generated ECMs in the storage unit** (137)." *ARRIS* at par. 0035 "8. The content delivery system of claim 2, wherein said **encryption renewal system transmits said encryption record and said encrypted control word corresponding to said second conditional access system to said caching system**, said caching system comprising one or more storage units for storing said encryption record and said encrypted control word." *ARRIS* at claim 8 "9. The content delivery system of claim 8, wherein said **encryption renewal system periodically regenerates said encrypted control word corresponding to said second conditional access system and transmits said regenerated encrypted control word to said caching system, wherein said caching system replaces said encrypted control word in said one or more storage units with said regenerated encrypted control word**." *ARRIS* at claim 9 "As shown in FIG. 4, **an interface (certificate exchange) based on a certificate authentication protocol may be used to allow the first ERS** (131-1) **to securely transfer to the second ERS** (131-2) **the information needed to uncover or decrypt the ER**. **The second ERS** (131-2) **may then generate the control word used to pre-encrypt the content and use its own encryption scheme to generate ECWs, ECMs, and/or other forms of the control word**." *ARRIS* at par. 0047 **B. US20050144478** "1. A content delivery system comprising: . . . **second decryption means for decrypting the encrypted content using the decrypted content key that is decrypted by the first decryption means**; . . . ." *Toshiba* at claim 1