PATROLL Winning Submission

U.S. Patent 8,667,304

U.S. Patent 8,667,304 ("*Videolabs*" or the "patent-at-issue") was filed on September 14, 2002 and claims priority on December 7, 2004. Claim 1 of the patent-at-issue is generally directed to a method and system for managing the presentation of content across different security domains, using a non-transitory machine-readable medium with executable instructions. This method involves a first conditional access server authenticating a client using a first authentication process and root of trust. Content from this client is then received by a second conditional access server, which processes the content and authorizes its own client to present this content based on authorization from the first server. The content is transmitted in an access-controlled format, specific to the second server, to its client across a second security domain. Importantly, the second server authenticates its clients using a second, independent authentication process and root of trust, distinct from those of the first server. Additionally, the second server is capable of substituting the first security domain with its own for the devices under its trust, ensuring secure content presentation across different domains.

The primary reference, U.S. Patent 7,706,540 ("*Fransdonk*"), was filed on January 31, 2006, and claims an earliest priority on June 16, 2000. The patent is directed to a method of secure content transmission, involving the generation of a set of session keys and the encryption of content using these keys to create encrypted content. This method ensures the encrypted content can be safely transmitted to a content destination, where it can be decrypted for use, provided the content destination has access to the set of session keys. This process aims to enhance the security and integrity of the transmitted content by ensuring only authorized parties can access and decrypt the content.

The primary reference, Patent App. 2004/0059913 ("*Jong*"), was filed on September 22, 2003, and claims priority on September 13, 2002. The patent is directed to a system and method for controlling access to digital content. This process involves sending a digital content request, receiving an authenticated request in response, and forwarding this authenticated request, along with specific delivery parameters, to a content repository. The repository, in turn, provides the requested encrypted digital content, which is then sent to a designated target device. This device is capable of decrypting the received content and rendering it for viewing. A notable aspect of this patent is that the encrypted digital content can be transmitted directly from the content repository to the target device, based primarily on the delivery parameters provided.

The secondary reference, U.S. Patent 9,419,951 ("*Felsher*"), was filed on December 1, 2014, and claims priority on March 23, 2001. The patent is directed to a system and method for secure communication between two parties through an intermediary. It involves receiving an identifier of desired information and accounting details for a transaction from the first party, transmitting the first party's identifier to the second party, and negotiating a comprehension function to obscure part of the information exchanged. To ensure security, the system uses asymmetric key encryption or direct key exchange for communication encryption. Furthermore, to protect the information at the second party, the data remains encrypted, with the intermediary

holding the decryption key. A secure method combines the decryption and a new encryption key for the second party to transcode the data, and the new decryption key is provided to the first party, enabling them to understand the transmitted information.

The secondary reference, the PCT application published as Publication WO 00/30323 ("*Schmeidler*") was filed on November 15, 1999 and claims an earliest priority on November 16, 1998. The patent is directed to a system for securely delivering on-demand content over broadband access networks. This system employs a dual-server approach alongside security mechanisms to prevent unauthorized access and execution of content by client processes. Specifically, it involves a content server, which stores a multitude of encrypted titles and is connected to the network, and an access server, also network-connected, that holds the network addresses of the titles along with the necessary keying and authorization data for decrypting and executing a title. A client application, running on a user's local computer system, must first obtain the address, keying, and authorization data from the access server. Only then can it retrieve a title from the content server and enable its execution on the local computer system, ensuring secure content delivery.

A sample claim chart comparing claim 1 of *Videolabs Inc* to *Fransdonk*, *Jong*, *Felsher*, and *Schmeidler* is provided below.

US8667304 ("*Videolabs*")	**A. US7706540** (*"Fransdonk"*) **B. US20040059913** (*"Jong"*) **C. US9419951** (*"Felsher"*) **D. WO2000030323** ("*Schmeidler*")
1.pre. A **non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content**,	**A. US7706540** "31. **A computer-readable medium storing a sequence of instructions** that, when executed by a machine, cause the machine to perform a method including: receiving time-varying session keys, the time-varying session keys encrypting content transmitted to a content destination; and **transmitting the time-varying session keys to the content destination, so as to enable the content destination, utilizing the time-varying session keys, to decrypt the encrypted content**." *Fransdonk* at Claim 31 **B. US20040059913** "In accordance with one embodiment of the present invention, **the components, process steps, and/or data structures may be implemented using various types of operating systems (OS), computing platforms, firmware, computer programs, computer languages, and/or general-purpose machines. The method can be run as a programmed process running on processing circuitry. The processing circuitry can take the form of numerous combinations of processors and operating systems, or a stand-alone device. The process can be implemented as instructions executed by such hardware, hardware alone, or any combination thereof. The software may be stored on a program storage device readable by a machine**." *Jong* at par. 0091 "**The present invention relates to the field of computer science**. More particularly, **the present invention relates to accessing for controlled delivery of digital content in a system for digital content access control**." *Jong* at par. 0010 **C. US9419951** "According to the present invention, **the security and privacy scheme of the present invention may be employed to convey content to users while ensuring compensation for rights-holders in the content.**" *Felsher* at col. 9:30-33

(cont.) 1.pre. A **non-transitory machine readable medium containing executable computer program instructions which when executed by a data processing system cause said system to perform a method to control a presentation of content**,	**D. WO2000030323** "The **Secure Content Delivery Platform** (SCDP) of the present invention delivers high-bandwidth executable content, on-demand, over broadband access networks." *Schmeidler* at p. 3 "According to an eleventh embodiment of the invention, **computer program product for use with a computer system operatively coupled over a computer network to one or more requestor processes, the computer program product comprising a computer usable medium having program code stored thereon comprising**: (a) program code configured to receive from a requestor process coupled to the network data identifying a selected title; (b) program code configured to receive payment information from the requestor process; (c) **program code configured to enable the requestor process to access selected portions of the title for downloading**; and (d) program code configured to allow execution of the title on a computer system while preventing installation of the title thereon." *Schmeidler* at p. 9
1.a. wherein **a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust**, the method comprising:	**A. US7706540** "The above-described aspect of the present invention may be utilized in one exemplary use scenario to secure highly confidential data that is delivered to, and stored on, a copy-protected device 408 (e.g., a user's computer). Depending upon the user's authentication mechanism, **a user may be required to utilize a hardware PKI token to authenticate the user to the copy-protected device 408 prior to obtaining access to the encrypted content**." *Fransdonk* at col. 35:60-67 "The **conditional access agent** 28 **interfaces with the conditional access server** 36 to query subscriptions. For this interface, **the conditional access agent** 28 **acts as the client**." *Fransdonk* at col. 17:9-11 "**Conditional access agents** 28 **are assigned a certain location identifier (ID)**, according to the physical region that they serve. Multiple conditional access agents 28 may be assigned to the same location ID. The **conditional access server** 36 **will map the conditional access agent ID to the appropriate region ID's to lookup the access criteria that are suitable for that agent**, if any." *Fransdonk* at col. 10:24-31

(cont.) 1.a. wherein **a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust**, the method comprising:	**B. US20040059913** "Turning now to FIG. 34, a detailed block diagram that illustrates a system for digital content access control in accordance with one embodiment of the present invention is presented. FIG. 34 illustrates using tokens to access digital content once the system has been initialized as described with respect to FIGS. 27-33. In operation, **user device** 3400 **sends a digital content request in the form of a URL to content provisioner** 3404 **via portal** 3458**. Download manager** 3414 **in provisioner manager** 3424 **receives the URL and communicates with content rights database** 3422 **to verify whether the user** 3402 **is authorized to access the digital content associated with the URL.**" *Jong* at par. 0199 "If the user 505 that made the request 560 is authorized to access the digital content associated with the request 560, issuer 585 issues an authenticator such as a token or the like and **provisioner manager** 545 **sends an authenticated digital content request** 565 **based at least in part on the authenticator to content repository** 520. **Repository manager** 555 **in content repository** 520 **receives the authenticated digital content request** 565 **and communicates with acceptor** 580 **and content database** 550 **to determine whether the authenticated digital content request** 565 **is valid**. The authenticated digital content request 565 is valid if the digital content specified by the authenticated digital content request is associated with the authenticator portion of the authenticated digital content request. If the authenticated digital content request 565 is valid, repository manager 555 returns the digital content 570 associated with the authenticated digital content request 565." *Jong* at par. 0123 "In operation, user device 5200 sends a digital content request 5250 to content provisioner 5252. according to one embodiment of the present invention, the digital content request 5250 is based at least in part on information received from content provisioner 5252. This information may comprise, by way of example, an indication of one or more services available to user 5205. **Provisioner manager** 5275 **in content provisioner** 5252 **receives the digital content request** 5250 **and communicates with content rights database** 5215 **to determine whether the user** 5205 **that made the request** 5250 **is authorized to access the digital content associated with the request** 5250." *Jong* at par. 0239

(cont.) 1.a. wherein **a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust**, the method comprising:	"**User device** 5200 **receives the authenticated digital content request** 355 **and then sends the authenticated digital content request** 5260 **to a content repository** 5282. **Repository manager** 5266 **in content repository** 5282 **receives the authenticated digital content request** 5282 **and communicates with acceptor** 5264 **and content database** 5290 **to determine whether the authenticated digital content request** 5260 **is valid**." *Jong* at par. 0240 **C. US9419951** "According to the present invention, **the user's "role" may be checked for consistency with a set of role-based usage rules. The reported role may be accepted, or verified with resort to an authentication database. Based on the role of the user and the identification of the content, the authority of the user to receive records may be determined**." *Felsher* at col. 9:62-67 "In order to increase portability, physical records, especially archives, may be stored physically or logically outside the source institution. Thus, limitations of access and bandwidth imposed by a public network gateway for an institution do not impede information transfer. **Authorizations, as distinct from the information sought to be communicated, are verified on-line, and may involve access to the source institution, but typically command substantially lower bandwidth requirements.**" *Felsher* at col. 14:30-38 "The **User** 20 **initiates the transaction by contacting the Intermediary** 10, **which typically maintains an** Accounting Database 11, a transaction log12, an **Authentication Database** 13, and a Secure Private Key Database 14."*Felsher* at col. 20:12-15 "The **Authentication Database** 13 **may**, for example, **provide a means for definitively identifying the User** 20, and/or, in the case of a medical record, the identity of the patient who consults the User 20, who is, for example, a health care professional. **This identification may be based on a Public Key Infrastructure, biometric identifiers, passwords and/or personal identification numbers (PIN), or other known means.** The Intermediary 10 may therefore provide a persistent association of the User 20 and/or a patient in its records, which facilitates accounting, application of rules, recalling of data from a database, etc." *Felsher* at col. 20:27-37

(cont.) 1.a. wherein **a first conditional access server has authenticated a client of the first conditional access server through a first authentication process that used a first root of trust**, the method comprising:	**D. WO2000030323** "**While the RAFT authorization token gives an SCDP client access to a title's briq, the SCDP client must still unpack, e.g. decompress and decrypt, the briq to gain access to the title's file data**." *Schmeidler* at p. 5 "Upon completion of the purchase negotiation, SCDP client software running on the user's PC obtains **an authorization token and keying material from a Conditional Access Server (CAS). The token authorizes the client process to run the selected title from a network file server accessible across the broadband network**. The data retrieved from the file server is encrypted. The SCDP client process uses the keying material provided by the conditional access server to decrypt the data from the file server." *Schmeidler* at p. 3-4
1.b. **receiving**, **at a second conditional access server**, **content from the client of the first conditional access server in a first security domain**;	**A. US7706540** "FIG. 1 illustrates, at a high-level, the processing of content as it is communicated from a content provider 16, via a content distributor 20, to a content destination 22. **At the content provider** 16**, clear content** 24 **is encrypted utilizing, for example, a symmetric product key (or content key) to generate encrypted content** 26**. It will thus be appreciated that the content provider** 16 **will be particularly concerned about security pertaining to the product key as access to this key potentially allows for regeneration of the clear content** 24**.** The encrypted content 26 (or cipher text) is then communicated from the content provider 16, via the network 18, to the content distributor 20. A conditional access agent 28, which represents the interests of the content provider 16 at the remote content distributor 20, may perform a number of operations in a secure environment with respect to the encrypted content 26. In one embodiment, the conditional access agent 28 decrypts the encrypted content 26 to regenerate the clear content 24 within a secure environment, and watermarks the clear content for distribution to a specific content destination 22. Watermarked content 30 may then be distributed from the content distributor 20 via the network 18, to a conditional access client 48 at the content destination 22. In an alternative embodiment, the conditional access agent 28 at the content distributor 20 may re-encrypt the content with a public key of a copy-protected device at the content destination 22. In any event, the clear and watermarked content 30 is then available for viewing and consumption at the content destination 22." *Fransdonk* at col. 6:3-30

(cont.) 1.b. **receiving**, **at a second conditional access server**, **content from the client of the first conditional access server in a first security domain**;	"The conditional access client 48 may reside on a personal computer or on the secure device 46. Where the **conditional access client** 48 **resides on a personal computer it may**, for example, **launch responsive to the issuance of a request from a further client program (e.g., a browser) to access certain content**." *Fransdonk* at col. 7:12-16 "The **conditional access client** 48 **initiates a secure session with a conditional access agent** 28 **to request an order for the relevant content item**. **If the content item is not cached at the content distributor** 20 **as cached content**, **the conditional access agent** 28 **retrieves access criteria for the requested content item from the conditional access server** 36 and forwards a derived XML signing request to the conditional access client 48." *Fransdonk* at col. 9:6-13 **B. US20040059913** "**If the user** 505 **that made the request** 560 **is authorized to access the digital content associated with the request** 560**, issuer** 585 **issues an authenticator such as a token or the like and provisioner manager** 545 **sends an authenticated digital content request** 565 **based at least in part on the authenticator to content repository** 520. Repository manager 555 in content repository 520 receives the authenticated digital content request 565 and communicates with acceptor 580 and content database 550 to determine whether the authenticated digital content request 565 is valid. The authenticated digital content request 565 is valid if the digital content specified by the authenticated digital content request is associated with the authenticator portion of the authenticated digital content request." *Jong* at par. 0123 If the authenticated digital content request 565 is valid, **repository manager** 555 **returns the digital content** 570 **associated with the authenticated digital content request** 565. **Portal operator** 515 **receives the digital content** 570 and sends the digital content 575 to user device 500. **D. WO2000030323** "According to a first embodiment of the invention, a method for securely delivering content over a network comprises the steps of: (a) storing at least one title on a content server operatively coupled to the network, the title stored in unexecutable form; (b) storing on an access server operatively coupled to the network a location identifier of the title and data necessary to process the title into executable form; (c)

(cont.) 1.b. **receiving**, **at a second conditional access server**, **content from the client of the first conditional access server in a first security domain**;	**requiring a client process operatively coupled to the network to obtain the location identifier of the title from the access server prior to retrieving at least a portion of the title from the content server; and (d) requiring a client process to obtain from the access server the data necessary to process the portion of the title into executable form.**" *Schmeidler* at p. 6 "The **SCDP client**, which, in the illustrative embodiment, **includes a Windows Virtual Device Driver (VxD), services these requests by retrieving the requested blocks of briq data from the RAFT server**." *Schmeidler* at p. 4
1.c. **processing the content on the second conditional access server**;	**A. US7706540** "FIG. 1 illustrates, at a high-level, **the processing of content as it is communicated from a content provider** 16**, via a content distributor** 20**, to a content destination** 22**.** At the content provider 16, clear content 24 is encrypted utilizing, for example, a symmetric product key (or content key) to generate encrypted content 26. It will thus be appreciated that the content provider 16 will be particularly concerned about security pertaining to the product key as access to this key potentially allows for regeneration of the clear content 24. **The encrypted content** 26 **(or cipher text) is then communicated from the content provider** 16**, via the network** 18**, to the content distributor** 20**. A conditional access agent** 28**, which represents the interests of the content provider** 16 **at the remote content distributor** 20**, may perform a number of operations in a secure environment with respect to the encrypted content** 26**. In one embodiment, the conditional access agent** 28 **decrypts the encrypted content** 26 **to regenerate the clear content** 24 **within a secure environment, and watermarks the clear content for distribution to a specific content destination** 22. Watermarked content 30 may then be distributed from the content distributor 20 via the network 18, to a conditional access client 48 at the content destination 22. **In an alternative embodiment, the conditional access agent** 28 **at the content distributor** 20 **may re-encrypt the content with a public key of a copy-protected device at the content destination** 22. In any event, the clear and watermarked content 30 is then available for viewing and consumption at the content destination 22." *Fransdonk* at col. 6:3-30 "The **conditional access client 48 receives an OK** (assuming a positive authentication and verification) **from the**

(cont.) 1.c. **processing the content on the second conditional access server**;	**conditional access agent 28 using a regular HTTP message, optionally including the session key encrypted under the user public key**." *Fransdonk* at col. 19:7-11 "In a second embodiment, the content is encrypted and **a key will therefore be required by the conditional access client 48 in order to decrypt the content.** The socket proxy will now be a RTSP proxy to provide intelligent blocking to implement functionality such as Pay Per Time." Fransdonk at col. 18:63-67 **B. US20040059913** "**If the user** 505 **that made the request** 560 **is authorized to access the digital content associated with the request** 560**, issuer** 585 **issues an authenticator such as a token or the like and provisioner manager** 545 **sends an authenticated digital content request** 565 **based at least in part on the authenticator to content repository** 520. **Repository manager** 555 **in content repository** 520 **receives the authenticated digital content request** 565 **and communicates with acceptor** 580 **and content database** 550 **to determine whether the authenticated digital content request** 565 **is valid. The authenticated digital content request** 565 **is valid if the digital content specified by the authenticated digital content request is associated with the authenticator portion of the authenticated digital content request**." *Jong* at par. 0123 "If the authenticated digital content request 5260 is valid, **repository manager** 5266 **applies a cryptographic process to the master key, the token key, the target ID, and possibly one or more delivery parameters or other indications to create a session key. The cryptographic process may comprise encryption.** Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. **The repository manager** 5266 **then encrypts the digital content with the session key** and returns the encrypted digital content 5238 associated with the authenticated digital content request 5260." *Jong* at par. 0240 **D. WO2000030323** "According to a first embodiment of the invention, a method for securely delivering content over a network comprises the steps of: (a) storing at least one title on a content server operatively coupled to the network, the title stored in unexecutable form; (b) storing on an access server operatively

(cont.) 1.c. **processing the content on the second conditional access server**;	coupled to the network a location identifier of the title **and data necessary to process the title into executable form**; (c) requiring a client process operatively coupled to the network to obtain the location identifier of the title from the access server prior to retrieving at least a portion of the title from the content server; and (d) requiring a client process to obtain from the access server the data necessary to process the portion of the title into executable form." *Schmeidler* at p. 6
1.d. **authorizing a client of the second conditional access server to present content in accordance with authorization the second conditional access server received from the first conditional access server**;	**A. US7706540** "Specifically, **a content distributor** 20**, after performing the necessary authorization and verification procedures**, **may forward content that it has cached to a content destination** 22 **or, if such content has not been cached, may issue a request for the relevant content to a content provider** 16. For example, if the content comprises a live "broadcast", the content may be directly forwarded via the content distributor 20 to the content destination 22." *Fransdonk* at col. 5:55-62 "The **conditional access client** 48 **receives an OK (assuming a positive authentication and verification) from the conditional access agent** 28 using a regular HTTP message, optionally including the session key encrypted under the user public key." *Fransdonk* at col. 19:7-11 "**Upon appropriate authorization of a request, at the content distributor** 20 **and under control of the conditional access agent** 28, **the requested content is decrypted and at least one association operation performed on the content before it is forwarded to the content destination** 22**.**" *Fransdonk* at col. 21:5-9 **B. US20040059913** "**Upon successful user authentication**, **the digital content producer** 105-120 **may grant access to the digital content** 155-170**. Alternatively, the digital content producer** 105-120 **may issue a token that may be presented at a later time and redeemed in exchange for access to the digital content**." *Jong* at par. 0012 **C. US9419951** "In one embodiment, a user is required to identify the specific records sought, and therefore **the authorization matrix representing correspondence of record content and user role may be associated with each record, and verified by the data repository as a part of a local authentication**

(cont.) 1.d. **authorizing a client of the second conditional access server to present content in accordance with authorization the second conditional access server received from the first conditional access server**;	**process prior to transmitting any portion of a record. Thus, the matrix may represent a metadata format describing the content of the record and the level or type of authority of the User to access that record. This metadata may, of course, itself be privileged information**." *Felsher* at col. 10:1-10 **D. WO2000030323** "According to a eighth embodiment of the invention, in a server apparatus comprising a processor, memory and a network interface, the server apparatus connectable to one or more client processes a computer network, a method comprises: (a) receiving a token from a client process through the network interface, the token containing data identifying a time period and data uniquely identifying a title; **(b) determining whether the client process is authorized to access the title at a specific time;** (c) **if the client is authorized in step (b), accessing the memory and a title uniquely identified by the token; and (d) supplying to the client at least a portion of the title identified by the token**." *Schmeidler* at p. 8-9
1.e. **transmitting, from the second conditional access server to the client of the second conditional access server through a network connection in a second security domain, the content that is in an access controlled format that is specified by the second conditional access server**; and	**A. US7706540** "**Specifically, a content distributor** 20**, after performing the necessary authorization and verification procedures**, may **forward content that it has cached to a content destination** 22 **or, if such content has not been cached, may issue a request for the relevant content to a content provider** 16**. For example, if the content comprises a live "broadcast", the content may be directly forwarded via the content distributor** 20 **to the content destination** 22." *Fransdonk* at col. 5:55-62 "In one embodiment, the **conditional access agent** 28 **decrypts the encrypted content** 26 **to regenerate the clear content** 24 **within a secure environment, and watermarks the clear content for distribution** to a specific content destination 22. **Watermarked content** 30 **may then be distributed from the content distributor** 20 **via the network** 18, **to a conditional access client** 48 **at the content destination** 22." *Fransdonk* at col. 6:18-24 **B. US20040059913** "According to embodiments of the present invention, **a specialized servlet is specified in an authenticated digital content request such as a URL. The specialized servlet**

(cont.) 1.e. **transmitting**, **from the second conditional access server to the client of the second conditional access server through a network connection in a second security domain**, **the content that is in an access controlled format that is specified by the second conditional access server**; and	**handles the provisioning of digital content protected by authenticated digital content requests**." *Jong* at par. 0132 "If the user 505 that made the request 560 is authorized to access the digital content associated with the request 560, issuer 585 issues an authenticator such as a token or the like and provisioner manager 545 sends an authenticated digital content request 565 based at least in part on the authenticator to content repository 520. Repository manager 555 in content repository 520 receives the authenticated digital content request 565 and communicates with acceptor 580 and content database 550 to determine whether the authenticated digital content request 565 is valid. The authenticated digital content request 565 is valid if the digital content specified by the authenticated digital content request is associated with the authenticator portion of the authenticated digital content request. If the authenticated digital content request 565 is valid, repository manager 555 returns the digital content 570 associated with the authenticated digital content request 565. **Portal operator** 515 receives the digital content 570 and **sends the digital content** 575 **to user device** 500. " *Jong* at par. 0123 "If the authenticated digital content request 5260 is valid, repository manager 5266 applies a cryptographic process to the master key, the token key, the target ID, and possibly one or more delivery parameters or other indications to create a session key. The cryptographic process may comprise encryption. Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. **The repository manager** 5266 then encrypts the digital content with the session key and **returns the encrypted digital content** 5238 **associated with the authenticated digital content request** 5260. According to one embodiment of the present invention, **the encrypted digital content** 5265 **is returned to the user device** 5200 **that issued the authenticated digital content request** 5260. " *Jong* at par. 0240 **C. US9419951** "Thus, **the system according to the present invention provides a conduit for the authorized transmission of records, such as medical records, while maintaining the security of the records against unauthorized access. A preferred communications network is the Internet, a global**

(cont.) 1.e. **transmitting**, **from the second conditional access server to the client of the second conditional access server through a network connection in a second security domain**, **the content that is in an access controlled format that is specified by the second conditional access server**; and	**interconnected set of public access networks, employing standardized protocols. Thus, the records may be transmitted virtually anywhere on earth using a single infrastructure**. Alternately, private networks or virtual private networks may be employed. In fact, as the system according to the present invention gains ubiquity, a private network model would be preferred, in order to increase security and allow the system to be tuned to the types of data and quality of service demands made by users" *Felsher* at col. 7:62-67 through col. 8:1-7 "It is also noted that, while the process shown in FIG. 1 generally provides a **communication flow of information from the Data Repository** 30 **to the User** 20, this communication stream may also be reversed, allowing the User 20 to upload information to the Encrypted Database 31 of the Data Repository 30, using a set of User 20 and Intermediary 10 Session Keys and the User 20 Private Key." *Felsher* at col. 20:1-7 "In one scenario, the **Data Repository** 30 receives the information from the Intermediary 10, and **recalls the identified record from an Encrypted Database** 31." *Felsher* at col. 22:36-38
1.f. **wherein 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. US7706540** "The above-described aspect of the present invention may be utilized in one exemplary use scenario to secure highly confidential data that is delivered to, and stored on, a copy-protected device 408 (e.g., a user's computer). **Depending upon the user's authentication mechanism, a user may be required to utilize a hardware PKI token to authenticate the user to the copy-protected device** 408 **prior to obtaining access to the encrypted content**." *Fransdonk* at col. 35:60-67 "In conclusion, **it will be noted that two separate and distinct authentication processes are performed at blocks** 426-428 **and** 430**. Further, it will be noted that each of these separate authentication processes verify separate and distinct user device and copy-protected device information (e.g., separate device certificates)**. By separating the authentication processes, an authorized user, in one exemplary use scenario, is enabled to utilize a copy-protected device of a third party to request and view content, for which that particular user is authorized. For example, the user authentication device may comprise a smart card, PKI token,

(cont.) 1.f. **wherein 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	SIM card or the like, that may be inserted into a personal computer, STB, PDA, cell phone or the like of a third party, thus enabling the authorized user to request content via a third party's copy-protected device 408." *Fransdonk* at col. 34:38-53 "The conditional access client 48 may reside on a personal computer or on the secure device 46. Where the conditional access client 48 resides on a personal computer it may, for example, launch responsive to the issuance of a request from a further client program (e.g., a browser) to access certain content. The **conditional access client** 48 operates to communicate a public key of the secure device 46 to a conditional access agent 28 and also **performs user authentication to verify that a particular user is authorized to initiate a transaction**." *Fransdonk* at col. 7:12-22 "The **conditional access client** 48 **receives an OK (assuming a positive authentication and verification) from the conditional access agent** 28 using a regular HTTP message, optionally including the session key encrypted under the user public key." Fransdonk at col. 19:7-11 **B. US20040059913** "**FIGS.** 57A-57B **make clear that cryptographic process** 5658 of FIG. 56B **may be split into two sub processes: a first cryptographic process** 5702 **that uses a target ID** 5704 **and a master key** 5700 **to produce a target key** 5706**, and a second cryptographic process** 5708 **that uses the target key** 5706 **and a token key** 5710 **to produce a session key** 5712. The first cryptographic process 5702 may be part of an enrollment process, where the target key 5706 is created and communicated to the enrolled target device. A key exchange protocol may be used to communicate the target key to the target device. The target key may be stored on the target device for subsequent use in creating one or more session keys. Once enrollment has taken place, **the second cryptographic process** 5728 **may be applied to the target key** 5726 **stored on the target device, together with a token key** 5730 **to create a session key** 5732 **for use in cryptographically protecting digital content** 5738." *Jong* at par. 0266 "In operation, user device 500 sends a digital content request 560 to portal 530 operated by portal operator 515. Portal 530 receives the digital content request 560 and communicates with provisioner manager 545 in content provisioner 535. **Portal**

(cont.) 1.f. **wherein 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	530 **may also communicate with user device** 500 **to obtain user authentication data such as a password, PIN, biometric data or the like.** If the user device 500 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like. **Provisioner manager 545 receives the digital content request** 560 **and communicates with content rights database** 540 **to determine whether the user** 505 **that made the request** 560 **is authorized to access the digital content associated with the request** 560. If the user 505 that made the request 560 is authorized to access the digital content associated with the request 560, issuer 585 issues an authenticator such as a token or the like and provisioner manager 545 sends an authenticated digital content request 565 based at least in part on the authenticator to content repository 520. **Repository manager** 555 **in content repository** 520 **receives the authenticated digital content request** 565 **and communicates with acceptor** 580 **and content database** 550 **to determine whether the authenticated digital content request** 565 **is valid**." *Jong* at par. 0123 **D. WO2000030323** "Next, **CAS** 700 **transmits the activator as well as a RAFT token to the SCDP client**, as illustrated in procedural step 736. The **CAS** 700 **retrieves the RAFT token from database** 750." *Schmeidler* at p. 33
1.g. **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 configured to substitute the first security domain with the second security domain for the client devices under the second root of trust**.	**A. US7706540** "The above-described aspect of the present invention may be utilized in one exemplary use scenario to secure highly confidential data that is delivered to, and stored on, a copy-protected device 408 (e.g., a user's computer). Depending upon the user's authentication mechanism, **a user may be required to utilize a hardware PKI token to authenticate the user to the copy-protected device** 408 **prior to obtaining access to the encrypted content**." *Fransdonk* at col. 35:60-67 "**During delivery to a conditional access client** 48**, the conditional access agent** 28 **replaces the session keys encrypted with the product key (Sp) with session keys encrypted with a unique user key (Uk), instead of the product key (Sp). Specifically, prior to deliver to a conditional access client** 48**, the conditional access agent** 28 **decrypts the encrypted product key received from the conditional access server** 36 **utilizing the private key (or secret key) of the conditional access agent** 28**, decrypts the**

(cont.) 1.g. **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 configured to substitute the first security domain with the second security domain for the client devices under the second root of trust**.	**sequence of session keys encrypted with the product key, and then re-encrypts the sequence of session keys utilizing the unique user key (Uk).**" *Fransdonk* at col. 25:66-26:24 "Upon receiving a user request for access to content of a particular content provider 16 at a conditional access agent 28, **the conditional access agent** 28 **may reorder (or re-rank) the list of accepted gateways to leverage existing trust relationships between the content requestor and, for example, a content distributor** 20 **hosting the conditional access agent** 28." *Fransdonk* at col. 26:8-18 The **conditional access client** 48 operates to communicate a public key of the secure device 46 to a conditional access agent 28 and also **performs user authentication** to verify that a particular user is authorized to initiate a transaction." *Fransdonk* at col. 7:18-22 "The **conditional access client 48 interfaces with the secure device 46 at the content destination 22.** Example secure devices 46 are smart cards or e-Tokens. A **secure device** 46 **may utilize the PKCSH** 11 **interface to provided device independent**." *Frandsdonk* at col. 9:40-44 "The conditional access agent server 80 provides a server implementation of a conditional access agent 28 for the client/agent interface. **A conditional access client** 48 **uses this interface to connect to the conditional access agent server** 80 **to complete a secure XML-based transaction based on access criteria associated with a requested content item**." *Fransdonk* at col. 17:37-43 **D. WO2000030323** "With the contemplated invention, **activators are unique per client, per briq, per execution, i.e., each activator obtained from the CAS is different and usable for one time only thereby preventing the leveraging of a single, costly reverse engineering effort out to multiple users**." *Schmeidler* at p. 5