ANNEXURE B

Contents

1. PROJECT SCOPE

TITLE:	**Tokenised Virtual Video Delivery System and Method**
PRIORITY DATE:	Patent applications granted and/or published in "US, EP & AU" in the last 25 years & PCT applications filed in last 31 Months.
CLIENT REQUEST :	Perform an FTO search on "Tokenised Virtual Video Delivery System and Method"
TAXONOMY:	**Primary Features:** A. A system for programmable video assembly, comprising: 1. a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data; 1.1. wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data. 1.2. wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources. 1.3. further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples. 2. a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information; 2.1. wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse. 2.2. wherein the transaction metadata includes instructions for micro

	payments triggered by individual segment resolution events. 2.3. wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event. 3. a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer. 3.1. wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment. 3.2. wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion. 4. a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references; 4.1. wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session. 4.2. wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners. 4.3. wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.

2. EXECUTIVE SUMMARY

This report provides a Freedom to Operate (FTO) analysis for "Tokenised Virtual Video Delivery System and Method". The purpose of this analysis is to determine whether the production, sale, and use of "Tokenised Virtual Video Delivery System and Method" infringe upon any existing patents. Based on our analysis, we have identified several patents that may pose a risk to the commercialization of "Tokenised Virtual Video Delivery System and Method". The search is focused on patent applications published or granted in "provided jurisdiction" in the last 25 years or PCT applications filed in last 31 months.

Multiple searches were performed on different databases, such as Patseer, Patentscope, USPTO, ESPACENET, Free Patents Online, AusPat and Google Patents to extract relevant references. The identified references were categorized in 2 sub categories - Relevant References and Closely Related References based on the relevancy criteria discussed further in the report.

We have considered the following 2 patents as relevant references which may hinder free operations of the subject product in concerned market(s):
1. Published Patent **EP2791847B1**, entitled, "**Improving startup times of streaming digital media playback**".
2. Published Patent **US 8,595,778 B2**, entitled, "**User authentication in a content delivery network**".

3. RISK ASSESSMENT MATRIX (UTILITY):

3.1 RELEVANT REFERENCES:

TAXONOMY	EP2791847 B1	US 8,595,778 B2
A. **A system for programmable video assembly, comprising:**	YES	YES
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**	YES	NO
1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	NO	NO
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	NO	NO
1.3. **further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.**	NO	NO
2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;**	YES	YES

2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	NO	NO
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	NO	NO
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.**	YES	YES
3. **a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.**	NO	NO
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	NO	NO
3.2. **wherein the logged dereference events trigger a commercial ~~action selected from a group consisting of billing, royalty~~**	NO	NO

allocation, and advertising insertion.		
4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	YES	YES
4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	NO	NO
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	NO	NO
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	NO	NO

3.2 CLOSELY RELATED REFERENCES:

TAXONOMY	US 10,455,286 B2	US 10,349,103 B2	EP2832102 B1	US 11,792,458 B2	US 12,244,881 B2	US 12,111,892 B2	US20260039463A1
A. **A system for programmable video assembly, comprising:**	YES	YES	YES	YES	YES	YES	YES
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**	YES	NO	YES	NO	NO	NO	NO
1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	NO	NO	NO	NO	NO	NO	NO
1.2. **wherein the step of**	NO	NO	NO	NO	NO	NO	NO

resolving referenced media data involves issuing MDAT range requests to the remote media data sources.							
1.3. further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.	YES	NO	NO	NO	NO	NO	NO
2. a token issuance service, wherein the service configured to generate a cryptographic video token binding	YES	YES	YES	YES	YES	YES	YES
transaction, consent, and licensing information;							
2.1. wherein the token issuance service includes a unique session nonce in	NO	YES	NO	YES	YES	NO	YES

each generated token to prevent unauthorized resolution reuse.							
2.2. wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.	NO	NO	NO	NO	NO	NO	NO
2.3. wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the	NO	NO	YES	NO	NO	YES	YES

resolution event.							
3. a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.	YES	YES	YES	NO	YES	YES	NO
3.1. wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.	YES	YES	NO	NO	YES	NO	NO
3.2. wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation,	NO	NO	NO	NO	NO	NO	NO

and advertising insertion.							
4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	YES	YES	YES	YES	NO	YES	NO
4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	NO	NO	NO	YES	NO	NO	NO
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	NO	NO	NO	NO	NO	NO	NO
4.3. **wherein the system is**	NO	YES	NO	NO	NO	NO	NO

configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.							

4. RELEVANT REFERENCES (UTILITY):

REFERENCE – 1 | **EP2791847 B1** | **TITLE:** Improving startup times of streaming digital media playback
FILING DATE: DEC 12, 2012 | **PUBLICATION DATE:** APR 17, 2019 | **PRIORITY DATE:** DEC 14, 2011
CURRENT ASSIGNEE: NETFLIX INC
STATUS: GRANTED | **INFRINGEMENT RISK**: HIGH

RELEVANT TEXT:

TAXONOMY	EP2791847 B1
A. **A system for programmable video assembly, comprising:**	**A computer-implemented method (300) for a client device to obtain authorization to stream a requested media title, the method comprising:** **outputting, for display in a user interface (400), a plurality of media titles available for streaming playback;** prior to receiving a user request (308) to begin streaming playback of any of the plurality of media titles, retrieving, by operation of one or more computer processors, metadata (306, 510) associated with at least a first one of the plurality of media titles; upon receiving the request to play the first media title (520), generating, based at least in part on the metadata, a request for a license (310) authorizing playback of the first media title; and upon receiving the license (312, 540) for the first media title, beginning streaming playback (318, 550) of the first media title. **(Refer: Claim 1)** **Remark:** *Prior art claim discloses computer-implemented method or system for a client device to obtain authorization to stream a requested media title (i.e.,*

	programmable video).
1. **a virtualization engine, wherein the engine is** **configured to convert a rendered video file into a** **reference container by extracting metadata and removing media sample data;**	A computer-implemented method (300) for a client device to obtain authorization to stream a requested media title, the method comprising: **outputting, for display in a user interface (400), a plurality of media titles available for streaming playback;** **prior to receiving a user request (308) to begin streaming playback of any of the plurality of media titles, retrieving, by operation of one or more computer processors, metadata (306, 510) associated with at least a first one of the plurality of media titles;** upon receiving the request to play the first media title (520), generating, based at least in part on the metadata, a request for a license (310) authorizing playback of the first media title; and upon receiving the license (312, 540) for the first media title, beginning streaming playback (318, 550) of the first media title. **(Refer: Claim 1)** **The method of claim 6, wherein the metadata (306) further includes a stream header associated with the first media title, wherein the stream header includes one or more attributes associated with the first media title. (Refer: Claim 7)** **Remark:** *The prior art claim discloses one or more computer processors that extract or retrieve metadata associated with at least a first one of the plurality of media titles (i.e., video files). The metadata comprises a stream header, which includes one or more attributes associated with the first media title. Therefore, the rendered media (video file) is converted into a reference*

container.

1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	N/A
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	N/A
1.3. **further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.**	N/A
2. **a token issuance service, wherein the service configured** **to generate a cryptographic video token binding transaction, consent, and licensing information;**	A computer-implemented method (300) for a client device to obtain authorization to stream a requested media title, the method comprising: outputting, for display in a user interface (400), a plurality of media titles available for streaming playback; prior to receiving a user request (308) to begin streaming playback of any of the plurality of media titles, retrieving, by operation of one or more computer

	processors, metadata (306, 510) associated with at least a first one of the plurality of media titles; **upon receiving the request to play the first media title (520), generating, based at least in part on the metadata, a request for a license (310) authorizing playback of the first media title; and** **upon receiving the license (312, 540) for the first media title, beginning streaming playback (318, 550) of the first media title. (Refer: Claim 1)** The method of any one of the preceding claims, wherein **the metadata (306) includes a metadata header associated with the first media title, wherein the metadata header includes an authentication and authorization token, and stream metadata information. (Refer: Claim 6)** **Remark:** *The prior art claim discloses that when a user requests to play the first media title, the system generates a request for a license authorizing playback of the first media title based on the metadata; i.e., a token may be generated to bind licensing information to the playback authorization of the first media title. The license request essentially asks the server for permission to play the chosen title.*
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	N/A

2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as** **an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.**	A computer-implemented method (300) for a client device to obtain authorization to stream a requested media title, the method comprising: outputting, for display in a user interface (400), a plurality of media titles available for streaming playback; prior to receiving a user request (308) to begin streaming playback of any of the plurality of media titles, **retrieving, by operation of one or more computer processors, metadata (306, 510) associated with at least a first one of the plurality of media titles;** **upon receiving the request to play the first media title (520), generating, based at least in part on the metadata, a request for a license (310) authorizing playback of the first media title; and** **upon receiving the license (312, 540) for the first media title, beginning streaming playback (318, 550) of the first media title. (Refer: Claim 1)** **Remark:** *The prior art claim discloses that when a user requests to play the first media title (video), the system generates a request for a license authorizing playback of the first media title based on the metadata; i.e., a token may be generated to bind licensing information to the playback authorization of the first media title. The license request essentially asks the server for permission to play the chosen title. The license information functions*

	as a permission mechanism, serving as an authorization gatekeeper that enforces playback rights by providing the necessary cryptographic credentials.
3. **a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.**	N/A
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	N/A
3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.**	N/A

4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	A computer-implemented method (300) for a client device to obtain authorization to stream a requested media title, the method comprising: outputting, for display in a user interface (400), a plurality of media titles available for streaming playback; prior to receiving a user request (308) to begin streaming playback of any of the plurality of media titles, retrieving, by operation of one or more computer processors, metadata (306, 510) associated with at least a first one of the plurality of media titles; upon receiving the request to play the first media title (520), generating, based at least in part on the metadata, a request for a license (310) authorizing playback of the first media title; and **upon receiving the license (312, 540) for the first media title, beginning streaming playback (318, 550) of the first media title. (Refer: Claim 1)** **Remark:** *The prior art claim discloses that the system begins streaming playback of the first media title after receiving the license (successful validation). Therefore, it can be inferred that playback of the first media title (video) occurs on the playback environment.*
4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	N/A
4.2. **wherein the playback**	N/A

environment may function as a content wallet capable of managing multiple tokens from independent content owners.	
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

REFERENCE – 2 | **US 8,595,778 B2** | **TITLE:** User authentication in a content delivery network
FILING DATE: OCT 23, 2009 | **PUBLICATION DATE:** NOV 26, 2013 | **PRIORITY DATE:** NOV 12, 2008
CURRENT ASSIGNEE: SANDPIPER CDN LLC
STATUS: GRANTED | **INFRINGEMENT RISK**: HIGH

RELEVANT TEXT:

TAXONOMY	US 8,595,778 B2
A. **A system for programmable video assembly, comprising:**	**A computer-implemented method for authorizing delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the method comprising:** **receiving a request from the end user for delivery of the video stream to the end user across a network;** querying a subscription database associated with the content publisher; in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream; and performing at least one of: transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream. **(Refer: Claim 1)**

	Remark: *Prior art claim discloses a method (or system) for authorizing delivery of a video stream (programmable video assembly) to an end user.*
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**	N/A
1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	N/A
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	N/A
1.3. **further comprising an artificial intelligence orchestration layer configured to modify the**	N/A

sequencing instructions of the reference container without accessing raw media samples.	
2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;**	A computer-implemented method for authorizing delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the method comprising: **receiving a request from the end user for delivery of the video stream to the end user across a network;** **querying a subscription database associated with the content publisher;** **in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream; and** performing at least one of: transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream. **(Refer: Claim 1)** **Remark:** *The prior art claim discloses that when a user sends a request for delivery of a video stream to the network, a query is generated for a subscription database containing the content publisher's licensing information. The subscription database evaluates the licensing or subscription data to*

	determine whether the end user is authorized to access the requested video stream. Accordingly, the database may issue a token in the reply that binds the subscription or licensing information to the users requested video stream.
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	N/A
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the**	A computer-implemented method for authorizing delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the method comprising: **receiving a request from the end user for delivery of the video stream to the end user across a network;** **querying a subscription database associated with the content publisher;** **in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of**

necessary cryptographic permissions and binds governance logic to the resolution event.	**the video stream; and** **performing at least one of:** **transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and** **initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream. (Refer: Claim 1)** **Remark:** *The prior art claim discloses that when an end user submits a request for a video stream across a network, a query is generated to a subscription database associated with the content publisher. The database evaluates licensing or subscription information to determine whether the user is authorized to access the requested stream. Accordingly, the database may issue a token that binds the subscription or licensing information to the user's requested video stream and functions as an integrated authorization gatekeeper, enforcing access rights by providing the necessary cryptographic permissions for stream delivery.*
3. **a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token;** **further comprising logging**	N/A

each individual media dereference event to an auditable transaction layer.	
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	N/A
3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.**	N/A
4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	A computer-implemented method for authorizing delivery of a video stream to an end user, wherein the video stream is associated with a content publisher, the method comprising: receiving a request from the end user for delivery of the video stream to the end user across a network; querying a subscription database associated with the content publisher; in response, processing a reply from the subscription database to determine whether the end user has authorization to receive delivery of the video stream; and

	performing at least one of: transmitting a notification to the end user indicating that the end user is not authorized to receive delivery of the video stream based on the processing of the reply from the subscription database; and **initiating delivery of the video stream to the end user based on the processing of the reply from the subscription database, wherein the reply from the subscription database indicates the end user is authorized to receive delivery of the video stream. (Refer: Claim 1)** **Remark:** *The prior art claim discloses that the subscription database evaluates licensing or subscription information to determine whether the end user is authorized to access the requested video stream. When the database's reply indicates that the user is authorized, the requested video stream is delivered for playback, i.e., the playback environment dynamically assembles the video streams.*
4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	N/A
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content**	N/A

owners.	
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

5. CLOSELY RELATED REFERENCES (UTILITY):

REFERENCE – 3 | **US 10,455,286 B2** | **TITLE:** Protected media decoding system supporting metadata
FILING DATE: MAR 08, 2019 | **PUBLICATION DATE:** OCT 22, 2019 | **PRIORITY DATE:** DEC 23, 2014
CURRENT ASSIGNEE: Microsoft Technology Licensing LLC
STATUS: GRANTED | **INFRINGEMENT RISK**: MEDIUM

RELEVANT TEXT:

TAXONOMY	US 10,455,286 B2
A. **A system for programmable video assembly, comprising:**	**A computing device comprising:** **a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content;** an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder; a secure digital rights management component configured to **receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to** yield decoded video content rather than decoding of the video content including metadata; and a video decoder component configured to provide the extracted metadata and the decoded video content to an application for playback. **(Refer: Claim 13)** **Remark:** *The claim discloses a method for computing device to decode the*

	protected video content by the video decoder.
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**	A computing device comprising: a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content; **an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder;** a secure digital rights management component configured to receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to yield decoded video content rather than decoding of the video content including metadata; and a video decoder component configured to provide the extracted metadata and the decoded video content to an application for playback. **(Refer: Claim 13)** **Remark:** *The claim discloses a method for a computing device to decrypt protected video content, wherein an extraction component is configured to extract metadata from the video content and provide the extracted metadata to a video decoder without providing the video content (i.e., media sample data) to the video decoder. This means that the system first extracts the metadata and then provides the metadata to the video decoder without transmitting the video content itself.*

1.1.	**wherein the virtual video**	N/A

container retains ISO Base Media File Format box structures while being devoid of media sample data.	
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	N/A
1.3. **further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.**	A computing device comprising: a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content; an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder; **a secure digital rights management component configured to receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to yield decoded video content rather than decoding of the video content including metadata**; and a video decoder component configured to provide the extracted metadata and

	the decoded video content to an application for playback. **(Refer: Claim 13)** **Remark:** *The claim discloses a secure digital rights management system configured to decode already protected video content rather than raw video content. Since this step involves a modification of the process, it can be deduced that the system is capable of modifying certain instructions based on the requirements.*
2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;**	A computing device comprising: a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content; an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder; **a secure digital rights management component configured to receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to yield decoded video content rather than decoding of the video content including metadata;** and a video decoder component configured to provide the extracted metadata and the decoded video content to an application for playback. **(Refer: Claim 13)** **Remark:** *The claim discloses a secure digital rights management component that enforces rights and licensing of protected video content through decryption and re-encryption prior to decoding by the video decoder, wherein the*

	decryption and re-encryption of the video content are based on a key (i.e., a token). This means that the secure digital rights management component ensures authorized access to the content based on the key.
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	N/A
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds**	N/A

governance logic to the resolution event.	
3. **a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.**	A computing device comprising: a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content; an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder; **a secure digital rights management component configured to receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to yield decoded video content rather than decoding of the video content including metadata;** and a video decoder component configured to provide the extracted metadata and the decoded video content to an application for playback. **(Refer: Claim 13)** The computing device of claim 13, **the secure digital rights management component being further configured to decrypt the protected video content to obtain decrypted video content and re-encrypt the decrypted video content based on a key of the computing device prior to providing the decrypted video content to the video decoder. (Refer: Claim 18)** **Remark:** *The claim discloses a secure digital rights management component*

	that enforces rights and licensing of protected video content through decryption and re-encryption prior to decoding by the video decoder, wherein the decryption and re-encryption of the video content are based on a key (i.e., token). This ensures that the secure digital rights management component provides authorized access to the content based on the key, corresponding to the secure resolution of the content or data.
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	**A computing device** comprising: a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content; an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder; a secure digital rights management component configured **to receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to yield decoded video content** rather than decoding of the video content including metadata; and a video decoder component configured to provide the extracted metadata and the decoded video content to an application for playback. **(Refer: Claim 13)** **Remark:** *The claim discloses that a computing device is used to access raw data from a streaming link. Further, the device employs encryption and decryption methods to protect the video until access is required by a user. Therefore, it can be deduced that this method is carried out in a hardware-*

	attested trusted execution environment.
3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.**	N/A
4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	A computing device comprising: a media source component configured to obtain video content from a media source, the video content including metadata as well as protected video content; an extraction component configured to extract the metadata from the video content to obtain extracted metadata, extracting the metadata including removing the metadata from the video content, and provide the extracted metadata to a video decoder without providing the video content to the video decoder for processing by the video decoder; a secure digital rights management component configured to receive the video content with the metadata removed from the extracting and provide the protected video content to the video decoder for decoding of the protected video content to yield decoded video content rather than decoding of the video content including metadata; and **a video decoder component configured to provide the extracted metadata and the decoded video content to an application for playback. (Refer: Claim 13)**

	Remark: *The claim discloses that the video decoder provides the metadata and the decoded video content to an application for playback corresponding to assembly of video streams in real time.*
4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	N/A
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	N/A
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

REFERENCE – 4 | **US 10,349,103 B2** | **TITLE:** Systems and methods for systems and methods for securely streaming media content
FILING DATE: MAR 05, 2018 | **PUBLICATION DATE:** JUL 09, 2019 | **PRIORITY DATE:** JUL 01, 2008
CURRENT ASSIGNEE: Sling Media LLC
STATUS: GRANTED | **INFRINGEMENT RISK**: MEDIUM

RELEVANT TEXT:

TAXONOMY	US 10,349,103 B2
A. **A system for programmable video assembly, comprising:**	**A method for securely providing a media stream from a server device to a remote player via a communications network, the method comprising:** receiving, at the server device, a request for a connection from the remote player via the communications network; in response to the request for the connection, requesting an authorization credential from a separately located central server via the communications network to authorize a media streaming session, wherein the authorization credential is generated and provided by the central server to both of the remote player and the server device via the communications network; and establishing the media streaming session between the server device and the remote player over the communications network in response to successfully verify the generated authorization credential by the central server so as to securely provide the media stream from the server device to the remote player, wherein at least a portion of the media stream is encrypted based upon the authorization credential. **(Refer: Claim 1)** **Remark:** *The claim discloses a method for secure transmission of a media*

	stream (i.e. audio or video) from a server to a remote player.
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**	N/A
1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	N/A
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	N/A
1.3. **further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.**	N/A

2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;**	A method for securely providing a media stream from a server device to a remote player via a communications network, the method comprising: receiving, at the server device, a request for a connection from the remote player via the communications network; in response to the request for the connection, **requesting an authorization credential from a separately located central server via the communications network to authorize a media streaming session, wherein the authorization credential is generated and provided by the central server to both of the remote player and the server device via the communications network;** and establishing the media streaming session between the server device and the remote player over the communications network in response to successfully verify the generated authorization credential by the central server so as to securely provide the media stream from the server device to the remote player, wherein at least a portion of the media stream is encrypted based upon the authorization credential. **(Refer: Claim 1)** **Remark:** *The claim discloses that the system receives a request to establish a connection between a server device and a remote device. In response to the connection request, authorization credentials (i.e., tokens) are generated and provided to both the remote device and the server device.*
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	A method for securely providing a media stream from a server device to a remote player via a communications network, the method comprising: receiving, at the server device, a request for a connection from the remote player via the communications network; in response to the request for the connection, **requesting an authorization**

	credential from a separately located central server via the communications network **to authorize a media streaming session**, wherein the authorization credential is generated and provided by the central server to both of the remote player and the server device via the communications network; and establishing the media streaming session between the server device and the remote player over the communications network **in response to successfully verify the generated authorization credential** by the central server so as to securely provide the media stream from the server device to the remote player, **wherein at least a portion of the media stream is encrypted based upon the authorization credential**. **(Refer: Claim 1)**
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media** **payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the**	N/A

necessary cryptographic permissions and binds governance logic to the resolution event.	
3. **a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.**	A method for securely providing a media stream from a server device to a remote player via a communications network, the method comprising: receiving, at the server device, a request for a connection from the remote player via the communications network; in response to the request for the connection, requesting an authorization credential from a separately located central server via the communications network to authorize a media streaming session, wherein the authorization credential is generated and provided by the central server to both of the remote player and the server device via the communications network; and **establishing the media streaming session between the server device and the remote player over the communications network in response to successfully verify the generated authorization credential by the central server so as to securely provide the media stream from the server device to the remote player, wherein at least a portion of the media stream is encrypted based upon the authorization credential. (Refer: Claim 1)** **Remark:** *The claim discloses that upon establishing a session between a server device and a remote player, a successful verification of authorization credentials is performed to securely provide the media stream from the server device to the remote player. This corresponds to secure access upon successful validation of the authorization credentials (i.e., token).*

3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	**A method for securely providing a media stream** from a server device **to a remote player via a communications network**, the method comprising: receiving, at the server device, a request for a connection from the remote player via the communications network; **in response to the request for the connection, requesting an authorization credential from a separately located central server via the communications network to authorize a media streaming session**, wherein the authorization credential is generated and provided by the central server to both of the remote player and the server device via the communications network; and **establishing the media streaming session between the server device and the remote player over the communications network in response to successfully verify the generated authorization credential** by the central server so as to securely provide the media stream from the server device to the remote player, wherein at least a portion of the media stream is encrypted based upon the authorization credential. **(Refer: Claim 1)**
3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.**	N/A
4. **a playback environment, wherein the playback environment stores multiple**	A method for securely providing a media stream from a server device to a remote player via a communications network, the method comprising:

tokens and dynamically assembling video streams in real-time from authorized references;	receiving, at the server device, a request for a connection from the remote player via the communications network; in response to the request for the connection, requesting an authorization credential from **a separately located central server via the communications network to authorize a media streaming session**, wherein **the authorization credential is generated** and provided by the central server **to both of the remote player and the server device via the communications network**; and **establishing the media streaming session between the server device and the remote player over the communications network in response to successfully verify the generated authorization credentia**l by the central server so as to securely provide the media stream from the server device to the remote player, wherein at least **a portion of the media ~~stream is encrypted based upon the authorization credential~~**. **(Refer: Claim 1)**
4.1. **wherein the playback environment is configured to manage independent tokens ~~from multiple content owners~~ within a single session.**	N/A
4.2. **wherein the playback environment may function as a content wallet capable of ~~managing multiple tokens from~~ independent content owners.**	N/A

4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	A method for securely providing a media stream from a server device to a remote player via a communications network, the method comprising: receiving, at the server device, a request for a connection from the remote player via the communications network; in response to the request for the connection, requesting an authorization credential from a separately located central server via the communications network **to authorize a media streaming session**, wherein the authorization credential is generated and provided by the central server to both of the remote player and the server device via the communications network; and **establishing the media streaming session between the server device and the remote player** over the communications network **in response to successfully verify the generated authorization credential** by the central server so as to securely provide the media stream from the server device to the remote player, wherein at least a portion of the media stream **is encrypted based upon the authorization credential**. **(Refer: Claim 1)** 16. The central computerized authentication system of claim 13 further comprising **validating that the user is authorized to connect to the media streaming device**. **(Refer: Claim 16)** **Remark:** *The claim discloses that an authorization code is required between the remote player and the central server for streaming content. Further, the system validates whether the user is authorized to connect to the media streaming device based on the credentials. Therefore, it can be deduced that if the credentials are incorrect or if the user is no longer authorized to view the streaming, the system may disconnect the connection between the remote server and the remote device.*

REFERENCE – 5 | **EP2832102B1** | **TITLE:** Methods and Systems for Cryptographic Access Control of Video
FILING DATE: MAR 31, 2012 | **PUBLICATION DATE:** OCT 31, 2018 | **PRIORITY DATE:** MAR 31, 2012
CURRENT ASSIGNEE: INTEL CORPORATION
STATUS: GRANTED | **INFRINGEMENT RISK**: MEDIUM

RELEVANT TEXT:

TAXONOMY	EP2832102B1
A. **A system for programmable video assembly, comprising:**	**A method of cryptographic access control - CAC - of video, comprising:** - by a metadata generator (225), generating (1215) metadata, said metadata representing an access control policy - **ACP - associated with the video,** the ACP including authorization rules and cryptographic information associated with an encryption policy; - by an encryptor (220), encrypting (1220) the video into an encrypted video (230) according to said encryption policy; and - by an encoder (240), encoding (1225) said encrypted video (230) into an encoded video (130) with said authorization rules and said cryptographic information, said encoded video having multiple segments; **wherein the authorization rules and cryptographic information are intended for decrypting and rendering the encoded video, characterized in that said encoding includes encoding different time segments of the encrypted video with corresponding different authorization rules,** wherein the authorization rules take into account user specific access controls, including Motion Picture - MP - ratings, an MP rating being embedded in a predetermined segment of said encoded video (130), each segment including a

	different rating intended for a different type of users. **(Refer: Claim 1)** **Remark:** *The prior art claims a method of cryptographic access control (CAC) for video, in which the authorization rules and cryptographic information are used to decrypt and render the encoded video (programmable video assembly).*
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**	A method of cryptographic access control - CAC - of video, comprising: - **by a metadata generator (225), generating (1215) metadata, said metadata representing an access control policy - ACP - associated with the video, the ACP including authorization rules and cryptographic information associated with an encryption policy;** - by an encryptor (220), encrypting (1220) the video into an encrypted video (230) according to said encryption policy; and - by an encoder (240), encoding (1225) said encrypted video (230) into an encoded video (130) with said authorization rules and said cryptographic information, said encoded video having multiple segments; wherein the authorization rules and cryptographic information are intended for decrypting and rendering the encoded video, characterized in that said encoding includes encoding different time segments of the encrypted video with corresponding different authorization rules, wherein the authorization rules take into account user specific access controls, including Motion Picture - MP - ratings, an MP rating being embedded in a predetermined segment of said encoded video (130), each segment including a different rating intended for a different type of users. **(Refer: Claim 1)** **Remark:** *The prior art claims that the metadata generator (i.e., virtualization engine) generates metadata representing the access control policy (ACP) associated with the video. Accordingly, it can be inferred that the metadata*

	contains a reference container extracted from the video.
1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	N/A
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	N/A
1.3. **further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.**	N/A
2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and**	A method of cryptographic access control - CAC - of video, comprising: - **by a metadata generator (225), generating (1215) metadata, said metadata representing an access control policy - ACP - associated with the video, the ACP including authorization rules and cryptographic information associated with an encryption policy;**

licensing information;	**- by an encryptor (220), encrypting (1220) the video into an encrypted video (230) according to said encryption policy;** and **- by an encoder (240), encoding (1225) said encrypted video (230) into an encoded video (130) with said authorization rules and said cryptographic information, said encoded video having multiple segments;** **wherein the authorization rules and cryptographic information are intended for decrypting and rendering the encoded video,** **characterized in that said encoding includes encoding different time segments of the encrypted video with corresponding different authorization rules,** wherein the authorization rules take into account user specific access controls, including Motion Picture - MP - ratings, an MP rating being embedded in a predetermined segment of said encoded video (130), each segment including a different rating intended for a different type of users. **(Refer: Claim 1)** **Remark:** *The prior art claims that the metadata represents the access control policy (ACP), including authorization rules (licensing information) and cryptographic information associated with an encryption policy. Accordingly, it can be inferred that when the ACP includes cryptographic information, a cryptographic video token is also generated.*
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	N/A

2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates** **independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.**	A method of cryptographic access control - CAC - of video, comprising: - by a metadata generator (225), **generating (1215) metadata, said metadata representing an access control policy - ACP - associated with the video,** the ACP including authorization rules and cryptographic information associated with an encryption policy; - by an encryptor (220), encrypting (1220) the video into an encrypted video (230) according to said encryption policy; and - by an encoder (240), encoding (1225) said encrypted video (230) into an encoded video (130) with said authorization rules and said cryptographic information, said encoded video having multiple segments; wherein the authorization rules and cryptographic information are intended for decrypting and rendering the encoded video, characterized in that said encoding includes encoding different time segments of the encrypted video with corresponding different authorization rules, wherein the authorization rules take into account user specific access controls, including Motion Picture - MP - ratings, an MP

rating being embedded in a predetermined segment of said encoded video (130), each segment including a different rating intended for a different type

	of users. (Refer: Claim 1) **Remark:** *The prior art claim discloses that the encoder encodes the video with authorization rules and cryptographic information, which govern rendering on the user device. Since the access control policy (ACP) includes cryptographic information, the generation of cryptographic video tokens is encompassed. The ACP functions as an authorization gatekeeper independent of the media payload, enforcing access rights by providing the cryptographic permissions necessary for decryption and playback.*
3. **a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.**	A method of cryptographic access control - CAC - of video, comprising: - by a metadata generator (225), generating (1215) metadata, said metadata representing an access control policy - ACP - associated with the video, the ACP including authorization rules and cryptographic information associated with an encryption policy; - by an encryptor (220), encrypting (1220) the video into an encrypted video (230) according to said encryption policy; and - **by an encoder (240), encoding (1225) said encrypted video (230) into an encoded video (130) with said authorization rules and said cryptographic information, said encoded video having multiple segments;** **wherein the authorization rules and cryptographic information are intended for decrypting and rendering the encoded video, characterized in that said encoding includes encoding different time segments of the encrypted video with corresponding different authorization rules,** **wherein the authorization rules take into account user specific access**

	controls, including Motion Picture - MP - ratings, an Mp rating being embedded in a predetermined segment of said encoded video (130), each segment including a different rating intended for a different type of users. (Refer: Claim 1) **Remark:** *The prior art claim discloses that the encoder encodes the video along with authorization rules and cryptographic information, and that the video is rendered on the user device according to these rules. Since the access control policy (ACP) includes cryptographic information, the generation of cryptographic video tokens is also encompassed. Accordingly, video rendering on the device occurs only upon successful validation of the ACP, which enforces access rights through authorization rules and cryptographic permissions.*
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	N/A
3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.**	N/A
4. **a playback environment, wherein the playback**	A method of cryptographic access control - CAC - of video, comprising: - by a metadata generator (225), generating (1215) metadata, said metadata

environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;	representing an access control policy - ACP - associated with the video, the ACP including authorization rules and cryptographic information associated with an encryption policy; - by an encryptor (220), encrypting (1220) the video into an encrypted video (230) according to said encryption policy; and - by an encoder (240), **encoding (1225) said encrypted video (230) into an encoded video (130) with said authorization rules and said cryptographic information,** said encoded video having multiple segments; **wherein the authorization rules and cryptographic information are intended for decrypting and rendering the encoded video,** characterized in that said encoding includes encoding different time segments of the encrypted video with corresponding different authorization rules, **wherein the authorization rules take into account user specific access controls, including Motion Picture - MP - ratings, an MP rating being embedded in a predetermined segment of said encoded video (130), each segment including a different rating intended for a different type of users. (Refer: Claim 1)**
	Remark: *The prior art claim discloses that the encoder encodes the video along with authorization rules and cryptographic information, and that the video is rendered on the user device according to these rules. Accordingly, video rendering or playback (assembling video streams) occurs only upon successful validation of the access control policy (ACP).*

4.1. **wherein the playback environment is configured to manage independent tokens** N/A

from multiple content owners within a single session.	
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	N/A
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

REFERENCE – 6 | **US 11,792,458 B2** | **TITLE:** Managing concurrent content playback
FILING DATE: JUL 13, 2022 | **PUBLICATION DATE:** OCT 17, 2023 | **PRIORITY DATE:** SEP 11, 2018
CURRENT ASSIGNEE: COMCAST CABLE COMMUNICATIONS, LLC
STATUS: GRANT | **INFRINGEMENT RISK**: MEDIUM

RELEVANT TEXT:

TAXONOMY	US 11,792,458 B2
A. **A system for programmable video assembly, comprising:**	**A method comprising:** **receiving, by a user device and from a content server, an indication of a permission granting the user device access to a content asset;** **sending, by the user device and to the content server, a request for a segment of the content asset;** and receiving, by the user device, from the content server, and based on a determination by the content server that the number of permissions currently granted to the user device exceeds the number of desired concurrent communication sessions by the user device, an indication that access to the another segment of the content asset has been denied. **(Refer: Claim 1)** **Remark:** *Prior art claims method of the content asset (i.e., programmable video).*
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by**	N/A

extracting metadata and removing media sample data;	
1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	N/A
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	N/A
1.3. **further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.**	N/A
2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding**	A method comprising: **receiving, by a user device and from a content server, an indication of a permission granting the user device access to a content asset;** **sending, by the user device and to the content server, a request for a**

transaction, consent, and licensing information;	**segment of the content asset;** and **receiving, by the user device, from the content server, and based on a determination by the content server that the number of permissions currently granted to the user device exceeds the number of desired concurrent communication sessions by the user device, an indication that access to the another segment of the content asset has been denied. (Refer: Claim 1)** The method of claim 1, wherein **the indication of the permission is generated in response to receipt at the content server of a token associated with the user device. (Refer: Claim 3)** The method of claim 3, wherein **the token comprises information associated with at least one of an identifier of the user device and an identifier of the content asset**. **(Refer: Claim 4)** **Remark:** *Prior art claim discloses user device receives an indication of a permission granting access to a content asset (e.g., audio or video) from content server. The indication of the permission is generated in response to receipt at the content server of a token associated with the user device. Such permission enables the user device to access the requested content. From this, it can be inferred that the indication of permission grant may be based on licensing information and may include a token associated with such licensing information.*
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent**	A method comprising: receiving, by a user device and from a content server, an indication of a permission granting the user device access to a content asset; **sending, by the user device and to the content server, a request for a**

unauthorized resolution reuse.	**segment of the content asset;** and **receiving, by the user device, from the content server, and based on a determination by the content server that the number of permissions currently granted to the user device exceeds the number of desired concurrent communication sessions by the user device, an indication that access to the another segment of the content asset has been denied. (Refer: Claim 1)** **Remark:** *Prior art claims that when a user device requests a segment of a content asset, the content server determines whether the number of permissions currently granted to the user device exceeds the number of desired concurrent communication sessions. If the number of permissions exceeds the allowed concurrent sessions (say, the subscription only allows one stream at a time), the server denies access to the new segment request. From this, it can be inferred that each communication session operates as a unique session nonce, thereby ensuring that permissions are bound to distinct session instances and preventing unauthorized concurrent access or reuse.*
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates**	N/A

independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.	
3. a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.	N/A
3.1. wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.	N/A

3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.**	N/A
4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	A method comprising: receiving, by a user device and from a content server, **an indication of a permission granting the user device access to a content asset**; sending, by the user device and to the content server, a request for a segment of the content asset; and receiving, by the user device, from the content server, **and based on a determination by the content server that the number of permissions currently granted** to the user device exceeds the number of desired concurrent communication sessions by the user device, an indication that access to the another segment of the content asset has been denied. **(Refer: Claim 1)**
4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	A method comprising: receiving, by a user device and from a content server, **an indication of a permission granting the user device access to a content asset**; sending, by the user device and to the content server, a request for a segment of the content asset; and receiving, by the user device, from the content server, and based on a

	determination by the content server **that the number of permissions currently granted to the user device exceeds the number of desired concurrent communication sessions by the user device, an indication that access to the another segment of the content asset has been denied**. **(Refer: Claim 1)**
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	N/A
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

REFERENCE – 7 | **US 12,244,881 B2** | **TITLE:** Method and system for secure over-the-top live video delivery
FILING DATE: OCT 25, 2022 | **PUBLICATION DATE:** MAR 04, 2025 | **PRIORITY DATE:** JUN 23, 2011
CURRENT ASSIGNEE: Telefonaktiebolaget LM Ericsson AB
STATUS: GRANTED | **INFRINGEMENT RISK**: MEDIUM

RELEVANT TEXT:

TAXONOMY	US 12,244,881 B2
A. **A system for programmable video assembly, comprising:**	**A method for managing secure distribution of audio or video content, comprising:** **generating a series of content encryption keys for encrypting a single audio or video content item**, each content encryption key associated with a different portion of the single audio or video content item wherein client devices requesting the single audio or video content item is further provided with key expiration information usable by the client devices to identify transitions between portions of the single audio or video content item that use different ones of the content encryption keys; and providing the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item, the license server being operative to establish that a requesting client device is authorized to access the content item, the license server being further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established. **(Refer: Claim 1)** **Remark:** *The claim discloses that a system or method for secure distribution of audio or video content by securely delivering the content to the authorized client device.*

1. a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;	N/A
1.1. wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.	N/A
1.2. wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.	N/A
1.3. further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing	N/A

raw media samples.	
2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;**	A method for managing secure distribution of audio or video content, comprising: **generating a series of content encryption keys for encrypting a single audio or video content item,** each content encryption key associated with a different portion of the single audio or video content item wherein client devices requesting the single audio or video content item is further provided with key expiration information usable by the client devices to identify transitions between portions of the single audio or video content item that use different ones of the content encryption keys; and **providing the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item, the license server being operative to establish that a requesting client device is authorized to access the content item**, the license server being further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established. **(Refer: Claim 1)** **Remark:** *The claim discloses that the system generates content encryption keys (i.e., cryptographic video tokens), where each encrypted key is associated with a different portion or segment of the content. The encryption keys are provided to the license server, which contains the licensing information for decrypting the content. The license server establishes or checks whether the client requesting the content is*

	authorized and provides the encryption keys to the authorized client.
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	A method for managing secure distribution of audio or video content, comprising: **generating a series of content encryption keys for encrypting a single audio or video content item, each content encryption key associated with a different portion of the single audio or video content item** wherein client devices requesting **the single audio or video content item is further provided with key expiration information usable by the client devices to identify transitions between portions of the single audio or video content item that use different ones of the content encryption keys;** and providing the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item, the license server being operative to establish that a requesting client device is authorized to access the content item, **the license server being further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established. (Refer: Claim 1)** **Remark:** *The claim discloses that the system generates encryption keys for encrypting the content, wherein each encryption key is associated with a different portion of a single audio or video file. Each encryption key is further provided with key expiration information, meaning that once a key expires, the system generates a new key corresponding to a unique session. Further, upon token issuance for the unique session, the*

	encryption keys are provided to the license server, which securely delivers the content to the authorized client device to prevent unauthorized use.
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.**	N/A
3. **a secure resolution service, wherein the service dereferences remote media**	A method for managing secure distribution of audio or video content, comprising: generating a series of content encryption keys for encrypting a single

data upon successful validation of the cryptographic video token; further comprising logging each individual media dereference event to an auditable transaction layer.	audio or video content item, each content encryption key associated with a different portion of the single audio or video content item wherein client devices requesting the single audio or video content item is further provided with key expiration information usable by the client devices to identify transitions between portions of the single audio or video content item that use different ones of the content encryption keys; and **providing the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item,** the license server being operative to establish that a requesting client device is authorized to access the content item, **the license server being further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established.** **(Refer: Claim 1)** **Remark:** *The claim discloses that the system provides secure access to the content with the help of a license server, which provides the encryption keys only to client devices whose authorization to access the content has been established. This means that client devices validated for authorized access are allowed to decrypt the content media with the help of the encryption keys provided by the license server.*
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted**	A method for managing secure distribution of audio or video content, comprising: generating a series of content encryption keys for encrypting a single audio or video content item, **each content encryption key associated**

execution environment.	**with a different portion of the single audio or video content item wherein client devices requesting the single audio or video content item is further provided with key expiration information usable by the client devices** to identify transitions between portions of the single audio or video content item that use different ones of the content encryption keys; and **providing the content encryption keys to a license server for delivery to the client devices for use in decrypting the content item**, the license server being operative to establish that a requesting client device is authorized to access the content item, the license server being further operative to securely deliver the content encryption keys to a requesting client device whose authorization to access the content item has been established. **(Refer: Claim 1)** **Remark:** *The claim discloses that the encryption and decryption keys are transmitted to the user device. Since the user device receives the codes and is password-protected, it can be deduced that the method is restricted to a trusted hardware device.*
3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of** **billing, royalty allocation, and advertising insertion.**	N/A
4. **a playback environment,**	N/A

wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;	
4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	N/A
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	N/A
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

REFERENCE – 8 | [US 12,111,892 B2] | **TITLE:** Streamlined digital rights management
FILING DATE: APR 09, 2020 | **PUBLICATION DATE:** OCT 08, 2024 | **PRIORITY DATE:** APR 27, 2016
CURRENT ASSIGNEE: COMCAST CABLE COMMUNICATIONS, LLC
STATUS: GRANTED | **INFRINGEMENT RISK**: MEDIUM

RELEVANT TEXT:

TAXONOMY	US 12,111,892 B2
A. **A system for programmable video assembly, comprising:**	**A system comprising:** **a license server; and** **a content server configured to:** **negotiate, with the license server, a license associated with media content;** receive, from a user device, **a request to access the media content, wherein the request to access the media content comprises an indication of an authentication of the user device,** wherein the authentication of the user device is performed via a session between the user device requesting access and an authentication server that is associated with the content server; determine, based on the indication of the authentication, to grant access to the media content; and send, to the user device, a content grant comprising a content key, wherein the content key is embedded in a manifest associated with the media content, and wherein the content key is based on the license, and wherein the media content is delivered to the user device via a session different from the session

	between the user device and the authentication server. **(Refer: Claim 7)** **Remark:** *Prior art claims the system for accessing media content (programmable video assembly).*
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a reference container by extracting metadata and removing media sample data;**	N/A
1.1. **wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.**	N/A
1.2. **wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.**	N/A
1.3. **further comprising an artificial intelligence**	N/A

orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.	
2. **a token issuance service, wherein the service configured to generate a cryptographic video token binding transaction, consent, and licensing information;**	A system comprising: **a license server; and** **a content server configured to:** **negotiate, with the license server, a license associated with media content;** **receive, from a user device, a request to access the media content, wherein the request to access the media content comprises an indication of an authentication of the user device,** wherein the authentication of the user device is performed via a session between the user device requesting access and an authentication server that is associated with the content server; **determine, based on the indication of the authentication, to grant access to the media content; and** **send, to the user device, a content grant comprising a content key, wherein the content key is embedded in a manifest associated with the media content, and wherein the content key is based on the license, and wherein the media content is delivered to the user device via a session different from the session between the user device and the authentication server. (Refer: Claim 7)**

Remark: *Prior art claim discloses upon a user request, a content grant*

	comprising a content key (i.e., a cryptographic video token), embedded with the media content (video) and based on licensing information, is sent to the user device.
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	N/A
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds**	A system comprising: a license server; and a content server configured to: negotiate, with the license server, a license associated with media content; **receive, from a user device, a request to access the media content, wherein the request to access the media content comprises an indication of an authentication of the user device, wherein the authentication of the user device is performed via a session between the user device requesting access and an authentication server that is associated with the content server;**

governance logic to the resolution event.	determine, based on the indication of the authentication, to grant access to the media content; and send, to the user device, a content grant comprising a content key, wherein the content key is embedded in a manifest associated with the media content, and wherein the content key is based on the license, and wherein the media content is delivered to the user device via a session different from the session between the user device and the authentication server. (Refer: Claim 7) **Remark:** *The prior art claims that the authentication server, associated with the content server, grants access to media content based on successful authentication. If access is allowed, it provides a content key (cryptographic video token), included in the media's manifest file and generated from the license. After validation, the user device receives the content key, enabling decryption and access to the delivered media. Accordingly, the content key functions as an integrated authorization gatekeeper, enforcing access rights via cryptographic permissions.*
3. a secure resolution service, wherein the service dereferences remote media data upon successful validation of the cryptographic video token; further comprising logging each individual media transaction event to an	A system comprising: a license server; and a content server configured to: negotiate, with the license server, a license associated with media content; receive, from a user device, a request to access the media content, wherein the request to access the media content comprises an layer.

dereference
auditable

indication of an authentication of the user device, wherein the authentication of the user device is performed via a session between the user device requesting access and an authentication server that is

	associated with the content server; **determine, based on the indication of the authentication, to grant access to the media content;** and **send, to the user device, a content grant comprising a content key, wherein the content key is embedded in a manifest associated with the media content, and wherein the content key is based on the license, and wherein the media content is delivered to the user device via a session different from the session between the user device and the authentication server.** **(Refer: Claim 7)** **Remark:** *The prior art claims that the authentication server, associated with the content server, determines whether to allow access to media content based on successful authentication. If access is granted, it provides permission information including a content key (cryptographic video token), which is included in the media's manifest file and generated from the license. Accordingly, after successful authentication and validation, the user device receives the content key, enabling it to decrypt and access the delivered media content.*
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	N/A
3.2. **wherein the logged dereference events trigger a**	N/A

commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.	
4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	A system comprising: a license server; and a content server configured to: negotiate, with the license server, a license associated with media content; receive, from a user device, a request to access the media content, wherein the request to access the media content comprises an indication of an authentication of the user device, wherein the authentication of the user device is performed via a session between the user device requesting access and an authentication server that is associated with the content server; determine, based on the indication of the authentication, to grant access to the media content; and **send, to the user device,** a content grant comprising a content key, wherein the content key is embedded in a manifest associated with the media content, and wherein the content key is based on the license, and **wherein the media content is delivered to the user device via a session different from the session between the user device and the authentication server. (Refer: Claim 7)** **Remark:** *Prior art claims the media content is delivered to the user device for streaming the content based on the licence. So, it can be infer that if the content is play to the user device, the keys will stored.*

4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	N/A
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	N/A
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

REFERENCE – 9 | **US20260039463A1** | **TITLE:** Method for receiving content in user device over cdn
FILING DATE: OCT 10, 2025 | **PUBLICATION DATE:** FEB 5, 2026 | **PRIORITY DATE:** OCT 10, 2025
CURRENT ASSIGNEE: Nagravision SARL
STATUS: PENDING | **INFRINGEMENT RISK**: Medium

RELEVANT TEXT:

TAXONOMY	US20260039463A1
A. **A system for programmable video assembly, comprising:**	**A method, carried out by a content provider system, comprising** the steps of: receiving an access request to access a content from a user device; generating a session key for a communication session for receiving said content in the user device over a content delivery network, generating an access token including the session key in encrypted form; generating, by a DRM license server, a DRM license including the session key; and transmitting the access token and the DRM license to the user device. **(Refer: Claim 5)** **Remark:** *Prior art claims a method for content (audio or video) providing system.*
1. **a virtualization engine, wherein the engine is configured to convert a rendered video file into a**	N/A

reference container by extracting metadata and removing media sample data;	
1.1. wherein the virtual video container retains ISO Base Media File Format box structures while being devoid of media sample data.	N/A
1.2. wherein the step of resolving referenced media data involves issuing MDAT range requests to the remote media data sources.	N/A
1.3. further comprising an artificial intelligence orchestration layer configured to modify the sequencing instructions of the reference container without accessing raw media samples.	N/A
2. a token issuance service, wherein the service configured to generate a cryptographic	A method, carried out by a content provider system, comprising the steps of: receiving an access request to access a content from a user device; generating a session key for a communication session for receiving said content

video token binding transaction, consent, and licensing information;	in the user device over a content delivery network, **generating an access token including the session key in encrypted form;** **generating, by a DRM license server, a DRM license including the session key;** and **transmitting the access token and the DRM license to the user device. (Refer: Claim 5)** **Remark:** *The claim discloses that the system generates the access token which includes a session key and based on that a license is generated. Further, upon authorization, the key and content will be delivered to the user.*
2.1. **wherein the token issuance service includes a unique session nonce in each generated token to prevent unauthorized resolution reuse.**	A method, carried out by a content provider system, comprising the steps of: **receiving an access request to access a content from a user device;** **generating a session key for a communication session for receiving said content in the user device over a content delivery network,** **generating an access token including the session key in encrypted form;** generating, by a DRM license server, a DRM license including the session key; and transmitting the access token and the DRM license to the user device. **(Refer: Claim 5)** **Remark:** *The prior art claims that a session key is generated for communication between the user device and the content delivery network, and an access token (cryptographic video token) is generated that includes the session key. Accordingly, it can be inferred that each access token contains a*

	unique session key to prevent unauthorized reuse of the token.
2.2. **wherein the transaction metadata includes instructions for micro payments triggered by individual segment resolution events.**	N/A
2.3. **wherein the cryptographic video token may function as an integrated authorization gatekeeper that operates independently of the media payload by excluding media sample data and direct file paths, enforces the right to resolve by providing the necessary cryptographic permissions and binds governance logic to the resolution event.**	A method, carried out by a content provider system, comprising the steps of: receiving **an access request to access a content from a user device**; generating a session key for a communication session for receiving said content in the user device over a content delivery network, **generating an access token including the session key in encrypted form**; generating, by a DRM license server, a DRM license including the session key; and **transmitting the access token and the DRM license to the user device**. **(Refer: Claim 1)**
3. **a secure resolution service, wherein the service dereferences remote media data upon successful**	N/A

validation of the cryptographic

video token; further comprising logging each individual media dereference event to an auditable transaction layer.	
3.1. **wherein the secure resolution service is restricted to operating within a hardware-attested trusted execution environment.**	N/A
3.2. **wherein the logged dereference events trigger a commercial action selected from a group consisting of billing, royalty allocation, and advertising insertion.**	N/A
4. **a playback environment, wherein the playback environment stores multiple tokens and dynamically assembling video streams in real-time from authorized references;**	N/A

4.1. **wherein the playback environment is configured to manage independent tokens from multiple content owners within a single session.**	N/A
4.2. **wherein the playback environment may function as a content wallet capable of managing multiple tokens from independent content owners.**	N/A
4.3. **wherein the system is configured to terminate the video stream instantly upon the revocation of user consent parameters associated with the token.**	N/A

6. KEY STRINGS

PATSEER:

Sr. No.	Key Strategies
1	TAC:(((VIRTUAL* OR REFERENCE) W3 (ENGINE OR CONVERTER OR CONTAINER OR GENERATOR OR EXTRACTOR OR FILE OR COMPILER)) AND (CRYPTOGRAPHIC*) AND (VERIF* OR AUTHENTICATION OR ATTESTATION OR CONFIRMATION OR CHECK* OR VALID*)) AND TACD:(((VIRTUAL* OR REFERENCE) W3 (FILE OR DATA OR SAMPLE OR METADATA)) WS (VIDEO OR MEDIA OR RENDERED_VIDEO OR (PLAYBACK W2 FILE)))
2	TACD:(((VIRTUAL* OR REFERENCE) W3 (ENGINE OR CONVERTER OR CONTAINER OR GENERATOR OR EXTRACTOR OR FILE OR COMPILER)) AND (CRYPTOGRAPHIC* W3 TOKEN) AND (TOKEN W3 (VERIF* OR AUTHENTICATION OR ATTESTATION OR CONFIRMATION OR CHECK* OR VALID*))) AND TACD:(((VIRTUAL* OR REFERENCE) W3 (FILE OR DATA OR SAMPLE OR METADATA)) WS (VIDEO OR MEDIA OR RENDERED_VIDEO OR (PLAYBACK W2 FILE)))
3	TACD:(((VIRTUAL* OR REFERENCE) W3 (ENGINE OR CONVERTER OR CONTAINER OR GENERATOR OR EXTRACTOR OR FILE OR COMPILER OR POINTER)) AND ((CRYPTOGRAPHIC* OR SECURE OR DIGITAL OR AUTHORIZATION) W3 (TOKEN OR KEY OR IDENTIFIER OR TAG OR CODE OR MARKER)) AND ((TOKEN OR KEY OR IDENTIFIER OR TAG OR CODE OR MARKER) W3 (VERIF* OR AUTHENTICATION OR ATTESTATION OR CONFIRMATION OR CHECK* OR VALID*))) AND TACD:(((VIRTUAL* OR REFERENCE) W3 (FILE OR DATA OR SAMPLE OR METADATA)) WS (VIDEO OR MEDIA OR RENDERED_VIDEO OR (PLAYBACK W2 FILE))) AND PBD:[2000-01-01 TO 2026-02-24] AND AC:(H04N21/*)
4	TAC:((CRYPTOGRAPHIC* OR SECURE OR DIGITAL OR AUTHORIZATION) W3 (TOKEN OR KEY OR IDENTIFIER OR TAG OR CODE OR MARKER)) AND TACD:(((REMOV* OR DELET* OR ERAS* OR STRIP OR DISCARD OR CLEAR OR OMIT*) W3 ((VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL) W3 (FILE OR DATA OR SAMPLE OR ORIGINAL OR ACTUAL))) AND ((EXTRACT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR*

	OR ACQUIR*) W3 (METADATA OR ((TIMING OR SEQUENCING OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION))) AND PBD:[2000-01-01 TO 2026-02-24]
5	TAC:((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE) W4 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION OR STREAM*)) AND TAC:(((ENCRYPT* OR CRYPTOGRAPHIC*) W3 (REFERENCE OR LINK*)) OR ((LINK* OR TIME OR SEQUENCE) W3 (INFORMATION OR DATA)) OR METADATA OR TIMESTAMPS) AND TACD:(((REMOV* OR DELET* OR ERAS* OR STRIP OR DISCARD OR CLEAR OR OMIT*) W3 ((VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR AUDIO OR PICTURE OR IMAGE OR ACTUAL OR ORIGINAL OR PLAYBACK OR MOVIE) W3 (FILE OR DATA OR SAMPLE OR ORIGINAL OR ACTUAL))) AND ((EXTRACT* OR RETRIEV* OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*) W3 ((META_DATA OR ((TIMING OR SEQUENCING OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG* OR ATTRIBUTES OR ANNOTATION))) WS (VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR AUDIO OR PICTURE OR IMAGE OR MOVIE OR VIDEOTAPE)) AND APD:[2000-01-01 TO 2026-02-24] AND AC:(H04L65/60 OR H04N21/2368 OR H04N21/8547 OR H04N21/4341 OR H04N21/*)
6	TAC:(((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE) W4 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION OR STREAM*)) AND (DIGITAL_RIGHTS_MANAGEMENT OR DRM OR LICENS* OR (RIGHTS W2 MANAGEMENT) OR SUBSCRIPTION) AND (VERIF* OR AUTHENTICATION OR ATTESTATION OR CONFIRMATION OR CHECK* OR VALID*)) AND TAC:((((ENCRYPT* OR CRYPTOGRAPHIC*) W3 (REFERENCE OR LINK*)) OR ((LINK* OR TIME OR SEQUENCE) W3 (INFORMATION OR DATA)) OR METADATA OR TIMESTAMPS) W5 (VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR AUDIO OR PICTURE OR IMAGE OR ACTUAL OR ORIGINAL OR PLAYBACK OR MOVIE)) AND TACD:(((EXTRACT* OR RETRIEV* OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*) W3 ((METADATA OR ((TIMING OR SEQUENCING OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG* OR ATTRIBUTES OR ANNOTATION))) WS (VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR AUDIO OR PICTURE OR IMAGE OR MOVIE OR VIDEOTAPE)) AND APD:[2000-01-01 TO 2026-02-25] AND AC:(H04L65/60 OR

	H04N21/2368 OR H04N21/8547 OR H04N21/4341 OR H04N21/*)
7	TAC:(((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE) W4 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION OR STREAM*)) AND (DIGITAL_RIGHTS_MANAGEMENT OR DRM OR LICENS* OR (RIGHTS W2 MANAGEMENT) OR SUBSCRIPTION OR CONSENT) AND (VERIF* OR AUTHENTICATION OR ATTESTATION OR CONFIRMATION OR CHECK* OR VALID*)) AND TAC:((((ENCRYPT* OR CRYPTOGRAPHIC*) W3 (REFERENCE OR LINK*)) OR ((LINK* OR TIME OR SEQUENCE) W3 (INFORMATION OR DATA)) OR METADATA OR TIMESTAMPS) W5 (VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR AUDIO OR PICTURE OR IMAGE OR ACTUAL OR ORIGINAL OR PLAYBACK OR MOVIE)) AND APD:[2000-01-01 TO 2026-02-25] AND AC:(H04L65/60 OR H04N21/2368 OR H04N21/8547 OR H04N21/4341 OR H04N21/*)
8	TAC:((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR VOD OR (LIVE W2 STREAM*) OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL MEDIA") AND (DIGITAL_RIGHTS_MANAGEMENT OR DRM OR LICENS* OR (RIGHTS W2 MANAGEMENT) OR SUBSCRIPTION OR CONSENT) AND ((METADATA OR TIMESTAMPS OR LINK* OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION OR INDEX* OR POINTER) W5 (VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL MEDIA"))) AND ((REMOV* OR DELET* OR ERAS* OR STRIP OR DISCARD OR CLEAR OR OMIT*) W5 ((ORIGINAL OR ACTUAL OR CONTENT OR RENDER* OR PLAYBACK OR SAMPLE) W3 (VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR FILE OR DATA))) AND APD:[2000-01-01 TO 2026-02-25]
9	TAC:((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR VOD OR (LIVE W2 STREAM*) OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL MEDIA") AND (DIGITAL_RIGHTS_MANAGEMENT OR DRM OR LICENS* OR (RIGHTS W2 MANAGEMENT) OR SUBSCRIPTION OR CONSENT OR PAYMENT) AND ((METADATA OR TIMESTAMPS OR LINK* OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION OR INDEX* OR POINTER) W5 (EXTRACT*

	OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*))) AND TACD:((REMOV* OR DELET* OR ERAS* OR STRIP OR DISCARD OR CLEAR OR OMIT*) W5 ((ORIGINAL OR ACTUAL OR CONTENT OR RENDER* OR PLAYBACK OR SAMPLE) W3 (VIDEO OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR FILE OR DATA))) AND APD:[2004-01-01 TO 2026-02-26] AND AC:(H04L65/60 OR H04N21/2368 OR H04N21/8547 OR H04N21/4341 OR H04N21/* OR G06F21/602 OR H04N7/1675)
10	AC:((H04N21/2541 OR H04N21/4627 OR H04L2209/603 OR G06F21/10) AND (G06F21/602 OR H04N21/63345 OR H04N21/64715 OR H04N21/63345 OR H04N7/1675 OR H04N21/63345) AND (H04N21/23476 OR H04N21/23895 OR H04N21/234 OR H04N21/4405 OR H04N21/23412 OR H04L65/60 OR H04N21/2368 OR H04N21/4341)) AND TACD:(((RENDER* OR PLAYBACK OR PLAY* OR TRANSMIT* OR SEND*) W5 (VALIDATION OR CHECKING OR VERIF* OR AUTHENTICATION OR ATTESTATION OR CONFIRMATION OR CHECK*))) AND TACD:((METADATA OR TIMESTAMPS OR LINK* OR VIRTUAL OR BLUEPRINT OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER" OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION OR INDEX* OR POINTER) W5 (EXTRACT* OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ~~ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*)) AND APD:[2004-01-01 TO 2026-02-26]~~
11	AC:((H04N21/23476 OR H04N21/23895 OR H04N21/234 OR H04N21/4405 OR H04N21/23412 OR H04L65/60 OR H04N21/2368 OR H04N21/4341 OR H04N21/2347 OR H04N21/4405) AND (H04N21/835 OR H04N21/8547 OR H04L2209/603 OR G06F21/10 OR H04N21/4627 OR H04N21/2541)) AND TACD:(((RENDER* OR PLAYBACK OR PLAY* OR TRANSMIT* OR SEND*) W5 (VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL MEDIA")) WS (VALIDATION OR CHECKING OR VERIF* OR AUTHENTICATION OR ATTESTATION OR CONFIRMATION OR CHECK*)) AND TACD:((METADATA OR TIMESTAMPS OR LINK* OR VIRTUAL OR BLUEPRINT OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER" OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION OR INDEX* OR POINTER) W5 (EXTRACT* OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*)) AND

	APD:[2004-01-01 TO 2026-02-26]
12	TAC:(((VIRTUAL* OR REFERENCE OR METADATA OR "MEDIA DESCRIPTION") W5 (CONTAINER OR EXTRACTOR OR GENERAT* OR CREAT* OR ENGINE)) AND ((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR VOD OR LIVE OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL MEDIA") W5 (DELIVERY OR DISTRIBUT* OR BROADCAST* OR TRANSFER* OR TRANSMISSION OR TRANSMIT* OR STREAM*)) AND (LICENSING OR SUBSCRIPTION OR (USER W3 CONSENT) OR (USER W3 PERMISSION) OR (USER W3 APPROVAL)) AND (SESSION OR ((SESSION) W3 (IDENTIFIERS OR ID OR KEY OR MARKER))) AND (AUTHORIZATION OR VALID* OR VERIFICATION OR AUTHENTICATION)) AND APD:[2004-01-01 TO 2026-02-26]
13	TAC:(((VIRTUAL* OR REFERENCE OR METADATA OR "MEDIA DESCRIPTION") W5 (CONTAINER OR EXTRACTOR OR GENERAT* OR CREAT* OR ENGINE)) AND ((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR VOD LIVE OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL MEDIA") W5 (DELIVERY OR DISTRIBUT* OR BROADCAST* OR TRANSFER* OR TRANSMISSION OR TRANSMIT* OR STREAM*)) AND (LICENSING OR SUBSCRIPTION OR (USER W3 CONSENT) OR (USER W3 PERMISSION) OR (USER W3 APPROVAL)) AND (SESSION OR ((SESSION) W3 (IDENTIFIERS OR ID OR KEY OR MARKER))) AND (AUTHORIZATION OR VALID* OR VERIFICATION OR AUTHENTICATION)) AND APD:[2004-01-01 TO 2026-02-26]
14	TAC:((VERIF* OR VALID* OR AUTHORIZ* OR AUTHENTICAT* OR CHECK*) W5 ((TOKEN OR KEY OR CODE OR CODEPOINT OR PASSCODE OR (ACCESS W2 CODE) OR (SECURITY W2 ARTIFACT)) W4 (METADATA OR META_DATA OR (TIMING W2 DATA) OR TIME_STAMP OR TIMESTAMP))) AND TACD:((((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR ON_DEMAND_MEDIA OR VOD OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR "VISUAL MEDIA") W3 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION OR STREAM*)) OR (LIVE W2 STREAM*))) AND TACD:(SERVER OR HOST OR (SERVICE W2 PROVIDER) OR (MEDIA W3 CENTER) OR (CONTENT W3 PROVID*) OR ((DISTRIBUTION OR DELIVERY OR STREAM OR MEDIA OR MULTIMEDIA OR MULTI_MEDIA) W2 (SYSTEM OR HUB OR SERVICE OR FACILITY OR CENTER OR HOST))) AND LSC:(ACTIVE - GRANTED)

15	TAC:(((SERVER OR HOST OR (SERVICE W2 PROVIDER) OR (MEDIA W3 CENTER) OR (CONTENT W3 PROVID*) OR ((DISTRIBUTION OR DELIVERY OR STREAM OR MEDIA OR MULTIMEDIA OR MULTI_MEDIA) W2 (SYSTEM OR HUB OR SERVICE OR FACILITY OR CENTER OR HOST))) AND (((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR ON_DEMAND_MEDIA OR VOD OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR "VISUAL MEDIA") W3 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION OR STREAM*)) OR (LIVE W2 STREAM*)) AND ((VERIF* OR VALID* OR AUTHORIZ* OR AUTHENTICAT* OR CHECK*) W5 ((TOKEN OR KEY OR CODE OR CODEPOINT OR PASSCODE OR (ACCESS W2 CODE) OR (SECURITY W2 ARTIFACT)) W4 (METADATA OR META_DATA OR (TIMING W2 DATA) OR TIME_STAMP OR TIMESTAMP))))) AND LSC:(ACTIVE - GRANTED)
16	ALLCTOF(PNC:EP2832102B1 OR EP2791847B1 OR US2007118849A1 OR US2026039463A1 OR US10349103B2)
17	C:(((TOKEN OR KEY OR IDENTIFIER OR SIGN* OR CODE OR TICKET OR CODEPOINT OR PASSCODE) W6 (LICENS* OR SUBSCRIB* OR CONSENT OR "EXECUTION CONSTRAINTS" OR DRM OR "RIGHTS MANAGEMENT" OR RIGHTS OR PURCHAS*)) AND ((DELIVERY OR DISTRIBUTION OR BROADCAST OR TRANSFER OR TRANSMISSION OR STREAM*) W5 (VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA")) AND (AUTHENTICAT* OR VALID* OR VERIF* OR AUTHORIZ*)) AND TAC:(((METADATA OR META_DATA OR (TIMING W2 DATA) OR TIME_STAMP OR TIMESTAMP) W6 (VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA"))) AND PBD:[2000-01-01 TO 2026-03-02]
18	C:(((TOKEN OR KEY OR IDENTIFIER OR SIGN* OR CODE OR TICKET OR CODEPOINT OR PASSCODE) W6 (LICENS* OR SUBSCRIB* OR CONSENT OR "EXECUTION CONSTRAINTS" OR DRM OR "RIGHTS MANAGEMENT" OR RIGHTS OR PURCHAS*)) AND ((DELIVERY OR DISTRIBUTION OR BROADCAST OR TRANSFER OR TRANSMISSION OR STREAM*) W5 (VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA")) AND (AUTHENTICAT* OR VALID* OR VERIF* OR AUTHORIZ*)) AND AC:(H04N21/23476 OR H04N21/23895 OR H04N21/234 OR H04N21/4405 OR H04N21/23412 OR H04L65/60 OR H04N21/2368 OR H04N21/4341 OR H04N21/2347 OR H04N21/4405) AND AC:(H04L9/3268 OR H04N21/63345 OR G06F21/602 OR H04N21/63345 OR H04N7/1675) AND PBD:[2000-01-01 TO 2026-03-02]

19	AASN:((INTEL) OR (NETFLIX) OR APPLE OR (IMAGEPROOF) OR (IBM) OR (GOOGLE) OR (HCL W3 TECHNOLOGY) OR (GENETEC) OR (VIDAFAIR) OR (VERIZON) OR (AMAZON) OR (DIVX) OR (NAGRAVISION W3 SARL) OR (GENETEC) OR (ION W3 VIDEO) OR (MICROSOFT) OR ((WARNER W3 BROS) W3 ENTERTAINMENT) OR (SONY) OR (ERICSSON) OR (III W3 HOLDINGS) OR (SLING W3 MEDIA) OR (HANGZHOU W3 TAOPIAOPIAO W3 FILM)) AND TAC:(((EXTRACT* OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*) W5 (METADATA OR TIMESTAMPS OR LINK* OR VIRTUAL OR BLUEPRINT OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER" OR DESCRIPTION OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) W3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION OR INDEX* OR POINTER)) WS (VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR VOD LIVE OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL DATA")) AND PBD:[2005-01-01 TO 2026-02-26] AND AC:(H04N21/23476 OR H04N21/23895 OR H04N21/234 OR H04N21/4405 OR H04N21/23412 OR H04L65/60 OR H04N21/2368 OR H04N21/4341 OR H04N21/2347 OR H04N21/4405)
20	INV:((IAN W3 MALONEY) OR (KARANVIR W3 GREWAL) OR (DAVID W3 DURHAM) OR (PRASHANT W3 DEWAN) OR (XIAOZHU W3 KANG) OR (MEN W3 LONG) OR (CHRISTIAN W3 KAISER) OR (JEAN W3 MARIE W3 WHITE) OR (YUNG W3 HSIAO W3 LAI) OR (YANN W3 BIEBER) OR (YONGJUN W3 WU) OR (BALACHANDAR W3 SIVAKUMAR) OR (SHYAM W3 SADHWANI) OR (PADMANABHA W3 RAO) OR (RAN W3 LIU) OR (CHUANJI W3 TANG) OR (ZUOLONG W3 WANG) OR (YE W3 SUN) OR (KYONG W3 PARK) OR (MICHAEL W3 CHEN) OR (PIERRE W3 RACZ) OR (FREDERIC W3 RIOUX) OR (TING W3 TSENG) OR (PAWEL W3 JURCZYK) OR (SEAN W3 WATSON) OR (MATTHEW W3 DALCIN) OR (AARON W3 MARKING) OR (JEFFREY W3 LOTSPIECH) OR (KENNETH W3 GOELLER)) AND TAC:(((EXTRACT* OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*) W5 (META_DATA OR TIME_STAMPS OR ((TIMING OR SEQUENC*) W3 (DATA OR INFO* OR INSTRUCTIONS)))) AND (VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR VOD LIVE OR "MULTI MEDIA" OR (MOVING W2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL W2 RECORDING) OR FILM OR "VISUAL DATA")) AND PBD:[2000-01-01 TO 2026-02-27]

AUSPAT:

Sr. No.	Key Strategies
1	CLAIMS = (MEDIA OR MULTIMEDIA OR VIDEO) AND (TOKEN OR KEY) AND (AUTHORIZAT* OR VALID* OR VERIF* OR AUTHENT*) AND FILING DATE FROM 1/1/2006 TO 2/27/2026 AND DESCRIPTION = METADATA OR "META DATA" OR TIMESTAMP
2	CLAIMS = (MEDIA OR MULTIMEDIA OR VIDEO OR AUDIO OR SONG) AND (TOKEN OR KEY OR PASSCODE OR CODEPOINT) AND (AUTHORIZAT* OR VALID* OR VERIF* OR AUTHENT*) AND FILING DATE FROM 1/1/2006 TO 2/27/2026 AND DESCRIPTION = (METADATA OR "META DATA" OR TIMESTAMP) AND (CRYPTOGRAPHIC* OR ENCRYPT*) AND ("VIRTUAL /3/ CONTAINER" OR "REFERENCE /4/ FILE" OR "REFERENCE /4/ LINK")
3	CLAIMS = (MEDIA OR MULTIMEDIA OR VIDEO OR AUDIO OR SONG) AND (AUTHORIZAT* OR VALID* OR VERIF* OR AUTHENT*) AND FILING DATE FROM 1/1/2006 TO 2/27/2026 AND DESCRIPTION = (METADATA OR ""META DATA"" OR TIMESTAMP) AND (LICENS* OR SUBSCR*) AND (CRYPTOGRAPHIC* OR ENCRYPT*) AND (""VIRTUAL /3/ CONTAINER"" OR ""REFERENCE /4/ FILE"" OR ""REFERENCE /4/ LINK"")
4	CLAIMS = (MEDIA OR MULTIMEDIA OR VIDEO OR AUDIO OR SONG) AND (AUTHORIZAT* OR VALID* OR VERIF* OR AUTHENT*) AND (TOKEN OR KEY) AND (""DIGITAL RIGHTS MANAGEMENT"" OR DRM OR RIGHTS OR LICENS* OR SUBSCR*) AND FILING DATE FROM 1/1/2005 TO 2/27/2026

GOOGLE PATENTS:

Sr. No.	Key Strategies
1	TAC=((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE) NEAR5 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION)) TAC=(CRYPTOGRAPHIC NEAR4 (TOKEN OR KEY)) TAC=((VIDEO OR MULTIMEDIA OR AUDIOVISUAL) NEAR4 (SEGMENTS OR PARTS OR PORTIONS OR SECTIONS OR DIVISIONS OR DIVISIONS OR PIECES OR SLICES OR FRAGMENTS)) TAC=((VIRTUAL* OR REFERENCE) NEAR4 (CONTAINER OR FILE)) CPC=(H04N21/2541) OR CPC=(H04N21/23476) OR CPC=(H04N21/LOW) COUNTRY:US,EP,WO,AU AFTER:FILING:20050101
2	TAC=((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE) NEAR5 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION)) TAC=(CRYPTOGRAPHIC NEAR4 (TOKEN OR KEY)) TAC=((VIDEO OR MULTIMEDIA OR AUDIOVISUAL) NEAR4 (SEGMENTS OR PARTS OR PORTIONS OR SECTIONS OR DIVISIONS OR DIVISIONS OR PIECES OR SLICES OR FRAGMENTS)) CL=((VIRTUAL* OR REFERENCE) NEAR4 (CONTAINER OR FILE)) TAC=(STREAM*) COUNTRY:US,EP,WO,AU AFTER:FILING:20050101
3	TAC=((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE) NEAR5 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMISSION)) TAC=((VIDEO OR MULTIMEDIA OR AUDIOVISUAL) NEAR4 (SEGMENTS OR PARTS OR PORTIONS OR SECTIONS OR DIVISIONS OR DIVISIONS OR PIECES OR SLICES OR FRAGMENTS)) CL=((VIRTUAL* OR REFERENCE) NEAR4 (CONTAINER OR FILE)) TAC=(MEDIA NEAR3 STREAM*) TAC=((CRYPTOGRAPHIC OR SECURE OR AUTHORIZATION OR ENCRYPTED) NEAR4 (TOKEN OR KEY)) ~~COUNTRY:US,EP,WO,AU AFTER:FILING:20050101~~
4	TAC=((CRYPTOGRAPHIC OR ENCRYPT*) NEAR3 ("TOKEN" OR "KEY" OR PASSCODE OR CODE)) TAC=((CONTENT OR VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE OR "VISUAL MEDIA") OR "MOTION PICTURE" OR FOOTAGE) NEAR3 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMI* OR STREAM*)) TAC=((VIRTUAL* OR REFERENCE OR LINK* OR METADATA OR TIMESTAMPS OR "TIMING DATA" OR "TIMING INFORMATION") NEAR3 (CONTAINER OR EXTRACT*

	OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLAT* OR SEPARAT* OR CAPTUR* OR ACQUIR*)) CPC=(H04N21/2368) OR CPC=(H04L65/60) OR CPC=(H04N21/234) OR CPC=(H04N21/23895) OR CPC=(H04N21/2389) OR CPC=(H04N21/23476) CPC=(G06F21/10 OR H04N21/2541 OR H04N21/4627 OR H04L2209/603 OR G06F21/10 OR H04N21/64715 OR H04N21/63345 OR H04N7/1675 OR H04N21/63345) COUNTRY:WO,US,EP,AU AFTER:FILING:20050101
5	((CRYPTOGRAPHIC OR ENCRYPT*) NEAR3 ("TOKEN" OR "KEY")) (VIDEO) TAC=((VIRTUAL* OR REFERENCE) NEAR3 (CONTAINER OR FILE OR ENGINE OR DATA OR METADATA)) ASSIGNEE:NETFLIX ASSIGNEE:YOUTUBE ASSIGNEE:FACEBOOK ASSIGNEE:META
6	TAC=((CONTENT OR VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR ("VISUAL MEDIA") OR "MOTION PICTURE" OR FOOTAGE) NEAR3 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMI* OR STREAM*)) TAC=((VIRTUAL* OR LINK* OR TIMESTAMPS OR "TIMING DATA" OR "TIMING INFORMATION" OR BLUEPRINT OR URL OR "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER") NEAR3 (EXTRACT* OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE OR OMIT)) CPC=(H04N21/2368) OR CPC=(H04L65/60) OR CPC=(H04N21/234) OR CPC=(H04N21/23895) OR CPC=(H04N21/2389) OR CPC=(H04N21/23476) TAC=((SUCCESS* OR COMPLETE) NEAR4 (AUTHORIZATION OR VALIDATION OR VERIFICATION OR AUTHENTICATION)) COUNTRY:WO,US,EP,AU AFTER:FILING:20050101
7	TAC=((CONTENT OR VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR ("VISUAL MEDIA") OR "MOTION PICTURE" OR FOOTAGE) NEAR3 (DELIVERY OR DISTRIBUTION OR BROADCAST* OR TRANSFER* OR TRANSMI* OR STREAM*)) TAC=(((URL OR "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER") NEAR3 (EXTRACT* OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE OR OMIT)) NEAR6 (CONTENT OR VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR ("VISUAL MEDIA") OR "MOTION PICTURE" OR FOOTAGE)) TAC=((SUCCESS* OR COMPLETE) NEAR4 (AUTHORIZATION OR VALIDATION OR VERIFICATION OR AUTHENTICATION)) TAC=(CRYPTOGRAPHIC NEAR3 (VIDEO NEAR3 TOKEN)) COUNTRY:WO,US,EP,AU AFTER:FILING:20050101

8	TAC=((ON_DEMAND) NEAR3 (CONTENT OR VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR ("VISUAL MEDIA") OR "MOTION PICTURE" OR FOOTAGE)) TAC=(LICENSE OR SUBSCRIBE OR SUBSCRIPTION OR DRM OR "RIGHTS") TAC=(AUTHORIZ* OR VALIDAT* OR VERIF* OR AUTHENTICAT*) (TOKEN OR KEY OR CODEPOINT OR TICKET OR PASSCODE) TAC=("META DATA" OR METADATA) COUNTRY:WO,US,EP,AU AFTER:FILING:20050101

USPTO:

Sr. No.	Key Strategies
1	(((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA") NEAR4 (DELIVERY OR DISTRIBUTION OR BROADCAST$ OR TRANSFER$ OR TRANSMISSION OR STREAM$)) AND ("DIGITAL RIGHTS MANAGEMENT" OR DRM OR LICENS$ OR (RIGHTS NEAR2 MANAGEMENT) OR SUBSCRIPTION OR CONSENT) AND (TOKEN OR KEY OR ((SECURE OR CRYPTOGRAPHIC$ OR DIGITAL) NEAR4 (KEY OR TOKEN OR IDENTIFIER OR SIGN$)))).CLM. AND @AD>"20050101" AND (H04N21/23476 OR H04N21/23895 OR H04N21/234 OR H04N21/4405 OR H04N21/23412 OR H04L65/60 OR H04N21/2368 OR H04N21/4341).CPC.
2	(((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL NEAR2 RECORDING) OR FILM OR "VISUAL MEDIA") NEAR4 (DELIVERY OR DISTRIBUTION OR BROADCAST$ OR TRANSFER$ OR TRANSMISSION OR STREAM$)) AND ("DIGITAL RIGHTS MANAGEMENT" OR DRM OR LICENS$ OR (RIGHTS NEAR2 MANAGEMENT) OR SUBSCRIPTION OR CONSENT) AND ((METADATA OR TIMESTAMPS OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) NEAR3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION) NEAR5 (VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL NEAR2 RECORDING) OR FILM OR "VISUAL MEDIA"))).CLM. AND @AD>"20050101" AND ((H04N21/2541 OR H04N21/4627 OR H04L2209/603 OR G06F21/10) AND H04N21/$).CPC.

3	(((VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL NEAR2 RECORDING) OR FILM OR "VISUAL MEDIA") NEAR4 (DELIVERY OR DISTRIBUTION OR BROADCAST$ OR TRANSFER$ OR TRANSMISSION OR STREAM$)) AND ("DIGITAL RIGHTS MANAGEMENT" OR DRM OR LICENS$ OR (RIGHTS NEAR2 MANAGEMENT) OR SUBSCRIPTION OR CONSENT) AND ((METADATA OR TIMESTAMPS OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) NEAR3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION) NEAR5 (VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL NEAR2 RECORDING) OR FILM OR "VISUAL MEDIA"))).CLM. AND @AD>"20050101" AND (G06F21/602 OR H04N21/63345 OR H04N21/64715 OR H04N21/63345 OR H04N7/1675 OR H04N21/63345).CPC. AND (H04N21/$).CPC.
4	(((METADATA OR TIMESTAMPS OR ((TIMING OR SEQUENC* OR STRUCTURAL OR DESCRIPTIVE OR REFERENCE) NEAR3 (DATA OR INFO OR INSTRUCTIONS OR FILE)) OR TAG OR ATTRIBUTE OR ANNOTATION) NEAR5 (VIDEO OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA" OR (MOVING NEAR2 IMAGE) OR "MOTION PICTURE" OR FOOTAGE OR (CLIP) OR (VISUAL NEAR2 RECORDING) OR FILM OR "VISUAL MEDIA")) AND (TOKEN OR PASSCODE OR KEY OR ((SECURE OR CRYPTOGRAPHIC$ OR DIGITAL) NEAR4 (KEY OR TOKEN OR IDENTIFIER OR SIGN$)))).CLM. AND @AD>"20050101" AND ((H04N21/2541 OR H04N21/4627 OR H04L2209/603 OR G06F21/10) AND (H04N21/23476 OR H04N21/23895 OR H04N21/234 OR H04N21/4405 OR H04N21/23412 OR H04L65/60 OR H04N21/2368 OR H04N21/4341)).CPC.
5	(((METADATA OR TIMESTAMP OR "LINKING DATA" OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER" OR "MEDIA DESCRIPTION") NEAR3 (EXTRACT OR GENERATE OR RETRIEVE OR DERIVE OR OBTAIN OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE)) AND (CONSENT OR LICENSE OR "EXECUTION CONSTRAINTS" OR DRM OR "RIGHTS MANAGEMENT") AND ((RENDER OR PLAYBACK OR PLAY$) NEAR5 (VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA"))).CLM. AND (H04N21/$).CPC. AND @AD>"20050101"
6	(((METADATA OR TIMESTAMP OR "LINKING DATA" OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER" OR "MEDIA DESCRIPTION") NEAR3 (EXTRACT OR GENERATE OR RETRIEVE

	OR DERIVE OR OBTAIN OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE)) AND (CONSENT OR LICENSE OR "EXECUTION CONSTRAINTS" OR DRM OR "RIGHTS MANAGEMENT") AND (KEY OR CODEPOINT OR TOKEN)).CLM. AND @AD>"20050101"
7	(H04N21/23476 OR H04N21/23895 OR H04N21/234 OR H04N21/4405 OR H04N21/23412 OR H04L65/60 OR H04N21/2368 OR H04N21/4341 OR H04N21/2347 OR H04N21/4405).CPC. AND (((METADATA OR "META DATA") NEAR3 (EXTRACT$ OR OMIT$ OR GENERATE OR RETRIEVE OR DERIVE OR OBTAIN OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE)) AND (CONSENT OR (USER W3 CONSENT) OR (USER W3 PERMISSION) OR (USER W3 APPROVAL) OR SUBSCRIPTION)).CLM. AND @AD>"20050101"
8	(((VIDEO OR MEDIA) ADJ3 (STREAM OR PLAYBACK)) AND (TOKEN OR KEYS) AND (ENCRYT OR DECRYPT) AND (AUTHENTICAT* OR VALIDAT* OR AUTHORIZ* OR VERIF* OR VALID*)).CLMS.
9	((SYSTEM OR METHOD) ADJ3 (VIDEO_STREAM OR VIDEO_PLAYBACK)) AND (TOKEN OR (ENCRYPTION_KEY) OR KEYS OR (CONTENT_KEY)) AND (AUTHENTICAT* OR AUTHORIZ* OR VERIF* OR VALID*)
10	((VIDEO OR MEDIA OR CONTENT) AND (STREAM OR PLAYBACK OR RENDER) AND (((TOKEN OR (ENCRYPTION_KEY) OR (CONTENT_KEY) OR KEY) ADJ3 (VALID* OR AUTHENTICAT* OR APPROV* OR VERIF* OR AUTHORIZ*)) NEAR3(SESSION OR VIEW))).CLMS. AND(("713") AND ("380")).CLAS.
11	(("380" AND "725").CLAS.) AND ((VIDEO OR MEDIA) NEAR3((TOKEN OR KEY) ADJ3 (AUTHENTICAT* OR VALID* OR AUTHORIZ*)))
12	((380/232).CCLS.) AND ((VIDEO OR MEDIA) NEAR3(TOKEN OR KEY)) AND (PLAYBACK OR SREAM OR RENDER)
13	(((726/2) AND (726/9)).CCLS.) AND ((VIDEO OR MEDIA) AND (PLAYBACK OR SREAM OR RENDER) AND (METADATA OR REFERENCE OR FILE)) AND (380.CLAS.)
14	(725/114 AND 725/31).CCLS. AND ((VIDEO OR MEDIA OR CONTENT) NEAR3 (PLAYBACK OR RETRIEVAL OR

	DELIVERY OR STREAM OR RENDER)) AND (SECURE OR PROTECTED)
15	((380/210 AND 380/278 AND 380/277).CCLS.) AND ((VIDEO OR MEDIA OR CONTENT) NEAR3 (DELIVERY OR DISTRIBUTION OR PLAYBACK)) AND (SECURE OR PROTECTED OR AUTHORIZED) AND ((TOKEN OR KEY)) AND (ENCRYPT OR DECRYPT OR DECODE)

ESPACENET:

Sr. No.	Key Strategies
1	(CTXT=("VIRTUAL*" PROX/DISTANCE<3 "CONTAINER") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "CONTAINER") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "POINTER")) AND (FTXT=("REMOV*" PROX/DISTANCE<3 "AUDIOVISUAL") OR FTXT=("REMOV*" PROX/DISTANCE<3 "MEDIA") OR FTXT=("REMOV*" PROX/DISTANCE<3 "VIDEO") OR FTXT=("EXTRACT*" PROX/DISTANCE<3 "METADATA") OR FTXT=("EXTRACT*" PROX/DISTANCE<3 "TIMESTAMP") OR FTXT=("EXTRACT*" PROX/DISTANCE<3 "SEQUENC*")) AND (CTXT=("CRYPTOGRAPHIC" PROX/DISTANCE<3 "TOKEN") OR CTXT=("SECURE" PROX/DISTANCE<3 "TOKEN") OR CTXT=("CRYPTOGRAPHIC" PROX/DISTANCE<3 "KEY") OR CTXT=("DIGITAL" PROX/DISTANCE<3 "KEY") OR CTXT=("ACCESS" PROX/DISTANCE<3 "TOKEN") OR CTXT=("ACCESS" PROX/DISTANCE<3 "KEY"))
2	(FTXT=("REMOV*" PROX/DISTANCE<3 "AUDIOVISUAL") OR FTXT=("REMOV*" PROX/DISTANCE<3 "MEDIA") OR FTXT=("REMOV*" PROX/DISTANCE<3 "VIDEO") OR FTXT=("EXTRACT*" PROX/DISTANCE<3 "METADATA") OR FTXT=("EXTRACT*" PROX/DISTANCE<3 "TIMESTAMP") OR FTXT=("EXTRACT*" PROX/DISTANCE<3 "SEQUENC*")) AND (CTXT=("CRYPTOGRAPHIC" PROX/DISTANCE<3 "TOKEN") OR CTXT=("SECURE" PROX/DISTANCE<3 "TOKEN") OR CTXT=("CRYPTOGRAPHIC" PROX/DISTANCE<3 "KEY") OR CTXT=("DIGITAL" PROX/DISTANCE<3 "KEY") OR CTXT=("ACCESS" PROX/DISTANCE<3 "TOKEN") OR CTXT=("ACCESS" PROX/DISTANCE<3 "KEY")) AND (FTXT=("VIDEO" PROX/DISTANCE<3 "DELIVERY") OR FTXT=("VIDEO"

	PROX/DISTANCE<3 "TRANSMISSION"))
3	(CTXT=("VIRTUAL*" PROX/DISTANCE<3 "CONTAINER") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "CONTAINER") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "POINTER") OR CTXT=("VIRTUAL*" PROX/DISTANCE<3 "ENGINE") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "EXTRACTOR")) AND (CTXT=("CRYPTOGRAPHIC" PROX/DISTANCE<3 "TOKEN") OR CTXT=("SECURE" PROX/DISTANCE<3 "TOKEN") OR CTXT=("CRYPTOGRAPHIC" PROX/DISTANCE<3 "KEY") OR CTXT=("DIGITAL" PROX/DISTANCE<3 "KEY") OR CTXT=("ACCESS" PROX/DISTANCE<3 "TOKEN") OR CTXT=("ACCESS" PROX/DISTANCE<3 "KEY") OR CTXT ALL "TOKEN" OR CTXT ALL "KEY" OR CTXT ALL "CRYPTOGRAPHIC") AND PD >= "2005-01-01" AND (CLAIMS ANY "VIDEO" OR CLAIMS ANY "MULTIMEDIA" OR CLAIMS ANY "AUDIOVISUAL") AND (CTXT ANY "VALIDATION" OR CTXT=("AUTHORISATION" PROX/DISTANCE<3 "CHECK*") OR CTXT ALL "VERIF*" OR CTXT ALL "CONFIRMATION") FILTERS: COUNTRIES (FAMILY): US OR WO OR EP OR AU
4	(CTXT=("METADATA" PROX/DISTANCE<3 "VIDEO") OR CTXT=("TIMESTAMP" PROX/DISTANCE<3 "VIDEO") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "POINTER") OR CTXT=("VIRTUAL*" PROX/DISTANCE<3 "ENGINE") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "EXTRACTOR")) AND PD >= "2005-01-01" AND (CLAIMS ANY "VIDEO" OR CLAIMS ANY "MULTIMEDIA" OR CLAIMS ANY "AUDIOVISUAL" OR CLAIMS ANY "MEDIA" OR CLAIMS ANY "MOVIE") AND (CTXT ANY "VALIDATION" OR CTXT=("AUTHORISATION" PROX/DISTANCE<3 "CHECK*") OR CTXT ALL "VERIF*" OR CTXT ALL "CONFIRMATION") AND (FTXT ANY "DRM" OR FTXT = "DIGITAL RIGHTS MANAGEMENT" OR FTXT=("RIGHTS " PROX/DISTANCE<3 "MANAGEMENT ") OR FTXT ALL "LICENS*" OR FTXT ALL "SUBSCRIPTION") FILTERS: COUNTRIES (FAMILY): US OR WO OR EP OR AU
5	(CTXT ALL "METADATA" OR CTXT=("TIMESTAMP" PROX/DISTANCE<3 "VIDEO") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("SEQUENC*" PROX/DISTANCE<3 "DATA") OR CTXT=("TIMING" PROX/DISTANCE<3 "INFORMATION") OR CTXT=("MEDIA" PROX/DISTANCE<3 "DESCRIPTION") OR CTXT=("VIDEO" PROX/DISTANCE<3 "ATTRIBUTES") OR CTXT=("REFERENCE" PROX/DISTANCE<3 "DATA")) AND PD >= "2005-01-01" AND (CLAIMS ANY "VIDEO" OR CLAIMS ANY "MULTIMEDIA" OR CLAIMS ANY

	"AUDIOVISUAL" OR CLAIMS ANY "MEDIA" OR CLAIMS ANY "MOVIE") AND (CTXT ANY "VALIDATION" OR CTXT ALL "AUTHORISATION" OR CTXT ALL "VERIF*" OR CTXT ALL "CONFIRMATION" OR CTXT ALL "CHECK*") AND (FTXT ANY "DRM" OR FTXT = "DIGITAL RIGHTS MANAGEMENT" OR FTXT=("RIGHTS " PROX/DISTANCE<3 "MANAGEMENT ") OR FTXT ALL "LICENS*" OR FTXT ALL "SUBSCRIPTION") AND (CL =/LOW "H04N21/" AND CL ANY "H04N21/2541 H04N21/4627 H04L2209/603 G06F21/10") FILTERS: COUNTRIES (FAMILY): US OR WO OR EP OR AU
6	(CTXT=("VIRTUAL" PROX/DISTANCE<3 "CONTAINER") OR CTXT=("TIMESTAMP" PROX/DISTANCE<3 "VIDEO") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("SEQUENC*" PROX/DISTANCE<3 "DATA") OR CTXT=("TIMING" PROX/DISTANCE<3 "INFORMATION") OR CTXT=("MEDIA" PROX/DISTANCE<3 "DESCRIPTION") OR CTXT=("VIDEO" PROX/DISTANCE<3 "ATTRIBUTES") OR CTXT ALL "METADATA" OR CTXT ALL "TIMESTAMP") AND PD >= "2005-01-01" AND (CLAIMS ANY "VIDEO" OR CLAIMS ANY "MULTIMEDIA" OR CLAIMS ANY "AUDIOVISUAL" OR CLAIMS ANY "MEDIA" OR CLAIMS ANY "MOVIE" OR CLAIMS=("VISUAL" PROX/DISTANCE<3 "DATA")) AND (CTXT ANY "VALID*" OR CTXT ALL "AUTHORISATION" OR CTXT ALL "VERIF*" OR CTXT ALL "CONFIRMATION" OR CTXT ALL "AUTHENTICATION") AND (CLAIMS ANY "DRM" OR CLAIMS = "DIGITAL RIGHTS MANAGEMENT" OR CLAIMS=("RIGHTS " PROX/DISTANCE<3 "MANAGEMENT ") OR CLAIMS ALL "LICENS*" OR CLAIMS ALL "SUBSCRIPTION" OR CLAIMS ALL "PAYMENT" OR CLAIMS=("PURCHAS*" PROX/DISTANCE<3 "DATA") OR CLAIMS=("PURCHAS*" PROX/DISTANCE<3 "HISTORY")) AND (CL ANY "H04N21/8547 H04N21/4627" OR CL ANY "H04N21/23476 H04N21/23895 H04N21/234 H04N21/4405 H04N21/23412 H04L65/60 H04N21/2368 H04N21/4341 H04N21/2347 H04N21/4405") FILTERS: COUNTRIES (FAMILY): US OR WO OR EP OR AU
7	(CTXT=("VIRTUAL" PROX/DISTANCE<3 "CONTAINER") OR CTXT=("TIMESTAMP" PROX/DISTANCE<3 "VIDEO") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("SEQUENC*" PROX/DISTANCE<3 "DATA") OR CTXT=("TIMING" PROX/DISTANCE<3 "INFORMATION") OR CTXT=("MEDIA" PROX/DISTANCE<3 "DESCRIPTION") OR CTXT=("VIDEO" PROX/DISTANCE<3 "ATTRIBUTES") OR CTXT ALL "METADATA" OR CTXT ALL "TIMESTAMP") AND PD >= "2005-01-01" AND (CLAIMS ANY "VIDEO" OR CLAIMS ANY "MULTIMEDIA" OR CLAIMS ANY "AUDIOVISUAL" OR CLAIMS ANY "MEDIA" OR CLAIMS ANY "MOVIE" OR CLAIMS=("VISUAL" PROX/DISTANCE<3 "DATA")) AND (CTXT ANY "VALID*" OR CTXT ALL "AUTHORISATION" OR CTXT ALL "VERIF*" OR CTXT ALL "CONFIRMATION" OR CTXT ALL "AUTHENTICATION") AND (CLAIMS ANY "DRM" OR CLAIMS = "DIGITAL RIGHTS

	MANAGEMENT" OR CLAIMS=("RIGHTS " PROX/DISTANCE<3 "MANAGEMENT ") OR CLAIMS ALL "LICENS*" OR CLAIMS ALL "SUBSCRIPTION" OR CLAIMS ALL "PAYMENT" OR CLAIMS=("PURCHAS*" PROX/DISTANCE<3 "DATA") OR CLAIMS=("PURCHAS*" PROX/DISTANCE<3 "HISTORY")) AND (CTXT=("TOKEN" PROX/DISTANCE<3 "VIDEO") OR CTXT ALL "TOKEN" OR CTXT=("CRYPTOGRAPHIC" PROX/DISTANCE<3 "KEY") OR CTXT=("AUTHENTIC*" PROX/DISTANCE<3 "TOKEN") OR CTXT=("AUTHENTIC*" PROX/DISTANCE<3 "KEY") OR CTXT=("AUTHORISATION" PROX/DISTANCE<3 "POLICY")) AND (FTXT ANY "SESSION" OR CLAIMS ANY "RUNTIME") FILTERS: COUNTRIES (FAMILY): US OR WO OR EP OR AU
8	(CTXT ALL "METADATA" OR CTXT=("META" PROX/DISTANCE<3 "DATA") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("TIMING" PROX/DISTANCE<3 "INFORMATION") OR CTXT=("MEDIA" PROX/DISTANCE<3 "DESCRIPTION") OR CTXT=("VIDEO" PROX/DISTANCE<3 "ATTRIBUTES") OR CTXT ALL "URL" OR CTXT ALL "TIMESTAMP" OR CTXT = "UNIFORM RESOURCE IDENTIFIER" OR CTXT = "URI" OR CTXT = "UNIFORM RESOURCE LOCATOR") AND PD >= "2000-01-01" AND (CLAIMS ANY "VIDEO" OR CLAIMS ANY "MULTIMEDIA" OR CLAIMS ANY "AUDIOVISUAL" OR CLAIMS ANY "MEDIA" OR CLAIMS ANY "MOVIE" OR CLAIMS=("VISUAL" PROX/DISTANCE<3 "DATA")) AND (CTXT ANY "VALID*" OR CTXT ALL "AUTHORISATION" OR CTXT ALL "VERIF*" OR CTXT ALL "CONFIRMATION" OR CTXT ALL "AUTHENTICATION") AND (CL ANY "H04N21/835 H04N21/8547 H04L2209/603 G06F21/10 H04N21/4627 H04N21/2541" AND CL ANY "H04N21/23476 H04N21/23895 OR H04N21/234 OR H04N21/4405 H04N21/23412 H04L65/60 H04N21/2368 H04N21/4341 H04N21/2347 H04N21/4405") FILTERS: COUNTRIES (FAMILY): US OR WO OR EP OR AU
9	(CTXT ALL "METADATA" OR CTXT=("META" PROX/DISTANCE<3 "DATA") OR CTXT=("REFERENCE " PROX/DISTANCE<3 "FILE") OR CTXT=("TIMING" PROX/DISTANCE<3 "INFORMATION") OR CTXT=("MEDIA" PROX/DISTANCE<3 "DESCRIPTION") OR CTXT=("VIDEO" PROX/DISTANCE<3 "ATTRIBUTES") OR CTXT ALL "URL" OR CTXT ALL "TIMESTAMP" OR CTXT = "UNIFORM RESOURCE IDENTIFIER" OR CTXT = "URI" OR CTXT = "UNIFORM RESOURCE LOCATOR") AND PD >= "2000-01-01" AND (CLAIMS ANY "VIDEO" OR CLAIMS ANY "MULTIMEDIA" OR CLAIMS ANY "AUDIOVISUAL" OR CLAIMS ANY "MEDIA" OR CLAIMS ANY "MOVIE" OR CLAIMS=("VISUAL" PROX/DISTANCE<3 "DATA")) AND (CL ANY "H04N21/835 H04N21/8547 H04L2209/603 G06F21/10 H04N21/4627 H04N21/2541" AND CL ANY "H04N21/23476 H04N21/23895 OR H04N21/234 OR H04N21/4405 H04N21/23412 H04L65/60 H04N21/2368 H04N21/4341 H04N21/2347 H04N21/4405") AND

	(CLAIMS ANY "LICENS*" OR CLAIMS ANY "SUBSCRIB*") FILTERS: COUNTRIES (FAMILY): US OR WO OR EP OR AU

PATENTSCOPE:

Sr. No.	Key Strategies
1	EN_CL:(((VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA") NEAR4 (DELIVERY OR DISTRIBUTION OR BROADCAST OR TRANSFER OR TRANSMISSION OR STREAM*)) AND ("DIGITAL RIGHTS MANAGEMENT" OR DRM OR LICENS* OR (RIGHTS NEAR2 MANAGEMENT) OR SUBSCRIPTION OR CONSENT OR PAYMENT OR (PURCHASE NEAR2 HISTORY)) AND (TOKEN OR KEY OR ((SECURE OR CRYPTOGRAPHIC OR DIGITAL) NEAR4 (KEY OR TOKEN OR IDENTIFIER OR SIGN*))) AND ((METADATA OR TIMESTAMPS) NEAR3 (EXTRACT* OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE))) AND AD:[01.01.2005 TO 25.02.2026]
2	EN_CL:(((METADATA OR TIMESTAMPS OR "TIMING DATA" OR "TIMING INFORMATION" OR INDEX OR REFERENCE OR VIRTUAL OR BLUEPRINT OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER") NEAR3 (EXTRACT* OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE)) AND (CONSENT OR LICENSE OR "EXECUTION CONSTRAINTS")) AND AD:[01.01.2005 TO 25.02.2026] AND CLASSIF:(H04N21/835 OR H04N21/8547)
3	EN_CL:(((METADATA OR TIMESTAMPS) NEAR3 (EXTRACT* OR GENERAT* OR RETRIEVE OR DERIVE OR OBTAIN* OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE)) AND (TOKEN OR KEY OR ((SECURE OR CRYPTOGRAPHIC OR DIGITAL) NEAR4 (KEY OR TOKEN OR IDENTIFIER OR SIGN*))) AND AD:[01.01.2005 TO 25.02.2026]) AND EN_ALLTXT:(RENDER* NEAR4 (VIDEO OR STREAMS OR MEDIA OR MULTIMEDIA OR AUDIOVISUAL OR ("VISUAL DATA"))) AND CLASSIF:(H04N21/2541 OR H04N21/4627 OR H04L2209/603 OR G06F21/10 OR H04N21/*)

4	EN_CL:(((METADATA OR TIMESTAMP OR "LINKING DATA" OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER" OR "MEDIA DESCRIPTION") NEAR3 (EXTRACT OR GENERATE OR RETRIEVE OR DERIVE OR OBTAIN OR ISOLATE OR SEPARATE OR CAPTURE OR ACQUIRE)) AND (CONSENT OR LICENSE OR "EXECUTION CONSTRAINTS" OR DRM OR "RIGHTS MANAGEMENT") AND ((RENDER OR PLAYBACK OR PLAY*) NEAR5 (VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA"))) AND AD:[01.01.2005 TO 25.02.2026]
5	EN_CL:(((METADATA OR TIMESTAMP OR "LINKING DATA" OR URL "UNIFORM RESOURCE LOCATOR" OR URI OR "UNIFORM RESOURCE IDENTIFIER" OR "MEDIA DESCRIPTION") NEAR6 (LICENS* OR SUBSCRIB* OR CONSENT OR "EXECUTION CONSTRAINTS" OR DRM OR "RIGHTS MANAGEMENT")) AND ((RENDER OR PLAYBACK OR PLAY*) NEAR5 (VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA")) AND (AUTHENTICAT* OR VALID* OR VERIF* OR AUTHORIZ*)) AND AD:[01.01.2000 TO 02.03.2026]
6	EN_CL:(((TOKEN OR KEY OR IDENTIFIER OR SIGN OR CODE OR TICKET OR CODEPOINT OR PASSCODE) NEAR6 (LICENS* OR SUBSCRIB* OR CONSENT OR "EXECUTION CONSTRAINTS" OR DRM OR "RIGHTS MANAGEMENT" OR RIGHTS)) AND ((DELIVERY OR DISTRIBUTION OR BROADCAST OR TRANSFER OR TRANSMISSION OR STREAM*) NEAR5 (VIDEO OR CONTENT OR MULTIMEDIA OR AUDIOVISUAL OR MOVIE OR MEDIA OR "MULTI MEDIA")) AND (AUTHENTICATE OR VALID* OR VERIF* OR AUTHORIZATION)) AND AD:[01.01.2000 TO 02.03.2026] AND CLASSIF:(H04L9/3268 OR H04N21/63345 OR G06F21/602 OR H04N21/63345 OR H04N7/1675)

7. CLASSES

a. IPC: G06F21/10, H04L65/1069, H04L65/1101, H04L65/60, H04L65/611, H04N21/234, H04N21/2347, H04N21/2368, H04N21/266, H04N21/4405, H04N21/4627, H04N21/835, H04N21/8355, H04N21/8547;

b. CPC: G06F21/602, H04L2209/603, H04L9/3268, H04N21/23412, H04N21/23476, H04N21/23895, H04N21/2541, H04N21/4341, H04N21/63345, H04N21/64715, H04N7/1675;

b. USPC: 380/210, 380/229, 380/232, 380/277, 380/278, 713/168, 725/114, 725/31, 726/2, 726/9;

8. CONCLUSION

A total of 9 patents/patent applications were identified and reviewed. The following are the main findings:

2 patents were found to be an immediate infringement risk discklosing "Methods and systems for authorizing and controlling the delivery of video streams to end users. A client device extracts metadata, including stream headers, for requested media titles, which is used to generate license requests. Tokens may be issued to bind licensing or subscription information to playback authorization, enforcing rights via cryptographic credentials. The system validates the license or subscription data through a query to a subscription or licensing database, and upon successful authorization, the requested video stream is delivered for playback. This broadly covers controlled media delivery and enforcement of access rights based on licensing or subscription information."

1 patent application and 6 patents were found that are related to "Methods and systems for secure media access, transmission, and playback. Video and audio content is provided with metadata separated from protected content, which is decrypted using tokens or keys issued by DRM and license servers. Access is restricted to authorized users, with session-based permissions preventing concurrent misuse. Cryptographic access control policies govern decryption and playback independently of the media, and segment-specific encryption keys with expiration information enable secure, session-specific access. Licenses and cryptographic tokens embedded in media manifests act as integrated authorization gatekeepers". However, independent claims of such patents/applications claim some additional components which may not be the part of the subject invention.

9. REFERENCE CRITERIA

Reference Criteria	Categorization
Relevant References	In-force or Active patents/applications with claim(s) which completely overlaps key feature/s of the subject product.
Closely Related References	In-force or Active patents/applications with claim(s) which partially overlaps key feature/s of the subject product. (OR) Legally not In-force patents/applications with claim(s) which completely or partially overlaps primary key feature/s of the subject product.

10. DISCLAIMER

This report is work of analysis and interpretation of publicly available information on various free and paid online sources and should not be construed as a legal opinion.