

COMPLETE SPECIFICATION

**IMPROVED CONTENT DISTRIBUTION ON A RETAIL CARD
THROUGH ONLINE- OFFLINE INTEGRATION ON A SINGLE
PLATFORM SECURED BY AN INDIVIDUAL LICENCE**

The following statement is a full description of this invention including the best method of performing it known to me:

IMPROVED CONTENT DISTRIBUTION ON A RETAIL CARD THROUGH ONLINE- OFFLINE INTEGRATION ON A SINGLE PLATFORM SECURED BY AN INDIVIDUAL LICENCE

[0001] This disclosure presents an improved video content distribution system on a retail card through a unique online offline integration on a single platform. This document is split into the following subsections: field of the invention, background of the invention, detailed description of invention, claims, abstract, description of figures and finally figures.

FIELD OF THE INVENTION

[0002] This disclosure generally relates to package assemblies, systems and methods for card products such as gift cards, debit cards, credit cards, discount cards, pharmaceutical cards, and the like.

[0003] The present invention also relates to the field of interactive communication using recognition of Quick Response (QR) codes, including and more particularly, *individualized real-time two-way communication QR code* recognition via client's portable device including (but not restricted to) mobile phones, tablets and similar portable devices for distribution of original video content.

BACKGROUND OF THE INVENTION

[0004] Manufacturers and retailers label their products with hang-tag labels that include logos, brand names, sizes, colours, pricing, promotions, sweepstakes, and bar codes for scanning product at time of sale. Moreover, they need to provide detailed product information such as material composition to clients (this is often mandated by law, depending on the product). A typical hang-tag is a simple piece of card stock (which can be folded) and which is attached to a garment or other product by a "swift tack" (i.e., a lopped plastic fastener applied by a gun) or a string or cord threaded through the top of the tag. Current hang-tags are primarily informational or promotional. Current printed labels contain static information, limited to generic promotion of company brand, communicating essential information to clients such as product collection name, colour, style, size, and a bar code with limited information that is primarily scanned by cashiers. Marketers have used printed QR codes, MS Tags, and other scan-able URL directing codes extensively on printed magazine advertisements and billboards,

but the field of use for QR codes on product, samples, packaging, containers, tags, and labels has not been commercialized to cater to individual client needs.

[0005] The market for wallet friendly, business card sized products continues to grow. Providing tangible products in such a format provides for long term storage, easy portability and easy retrieval upon need. Secure transactions through such cards have become a norm in today's technologically advanced world.

[0006] In an unrelated industry of media content and delivery, there has been a significant push towards entirely digital content. Subscription based, online (only) video on demand platforms like Netflix and Amazon Prime dominate the market. Such distribution requires audience members to incur recurring payments for subscription. This is not convenient/preferred as consumption is limited over such services, especially when a consumer explores various content options. The reach of such subscription services is limited with economically challenged and people stuck with busy lifestyles, worldwide. As a result, an *ongoing need exists for an improved bridge between online content and the way it is delivered to the consumer*, as is addressed by the present disclosure.

[0007] *This invention solves the problem of recurring subscription and over reliance on digital only content through business card sized content management system.* The resultant system – a tangible card and its integration with secure proprietary online streaming makes a unique combination which is instantly appealing to millions of people around the world as it's a single easy transaction for a product, not a service.

DETAILED DESCRIPTION OF THE INVENTION

[0008] In the following description, numerous specific details are introduced to provide a thorough understanding of and enabling for, the embodiments described herein. One skilled in relevant art and equipped with technical knowledge, will appreciate that these embodiments can be practiced standalone but it's the combination of these systems and methods that sets it apart and this combination is critical for the final new inventive tangible product. Well-known structures or operations are not shown, or are not described in detail, to avoid obscuring aspects of the disclosed embodiments.

[0009] The present invention relates to and/or provides methods, systems, embodiments, and compositions of matter relating to combination of product, packaging with scannable quick

response codes for instant connection to mobile web, a new process for making them “interactive” for individualized consumption and back end systems to bring copyrighted media content to the consumer quickly.

[00010] Present disclosure is a standalone product or sample product that relates to a single integrated system which includes, in one embodiment, (a) a digitally created *interactive dual Quick Response (QR) code* pointing to (b) *proprietary online screen*, (c) *printed on a portable physical card of dimension 3.5 x 2 inches*, (d) *associated packaging of panels (of any material)*, one or plenty, in any dimension, (e) *a virtual digital media container* adapted to securely hold one or more digital content and (f) *delivered through proprietary secure steaming or storage medium methods*. The digital media playing system also includes a (g) *trusted media content* procured from copyrighted legitimate sources to play via the disclosed embodiment. The trusted media content, hosted in content database online, is securely streamed coupled with native Digital Rights Management (DRM) technologies and (h) *locked to one mobile device only with digital forensic watermarking as invoked by the QR code and unique digital signatures, post security verification*.

[00011] In another embodiment, a variation of the same without forensic watermarking and possibility of multiple content on the same integrated system is also covered in this disclosure.

[00012] In another embodiment, the combination of (a) – (g) is not restricted to display through physical cards only. Other physical options like (but not limited to) a ticket, article of clothing, 3-D object, or any other suitable article which includes digital video and/or audio content identification indicia thereon that visually identifies and remotely connects to the proprietary online system is also covered in this disclosure.

[00013] The system of an embodiment for supporting QR code recognition processing for interactive communication to media content (encrypted or decrypted) comprises of one client device and a virtual server. Each client of the system comprises of a scanner component along with corresponding or coupled scanning application configured to scan a QR code **110**. Each client is also configured to process information or data of the received QR code **110** by encoding, decoding, compressing, decompressing, encrypting, decrypting, and other data processing as appropriate to the data type being processed. Typically, but not necessarily, the client will be configured to decode QR code locally rather than transferring QR code to a mobile application for interpretation.

[00014] As is listed in figure 1, the first step is to **100** natively scan QR code **110** using the media playing device. **200** “Individualized” data packets pointing to unique QR code **110** are received by the media playing device and mobile web points the client to a secure proprietary online screen. This screen is part of a protected ecosystem for digital content as covered by this disclosure. **300** The client then enters their device identifier and an “individualized” password **310** as held by the tangible card on the online screen. The fed information uniquely interacts with the back-end content database registry and creates a unique “one-time password” (OTP) with validity of (m) minutes. **400** This OTP is delivered to the client via their mobile network. In the next step **500**, the client must enter the generated OTP (unique customer identifier) to activate the card. There is one and only one combination of QR code, OTP and password, termed as the digital signature **501**, that activates the card. **600** Successful identification sends secure content to the media playing device for its time restricted display **700**.

[00015] The innovative step as covered in this disclosure is the individualization of QR code such that it locks the client with a printed password on a tangible card, a unique one-time generated password with the client’s mobile number to present an offline bridge to an online content for streaming or download. This novel way of integration between offline physical presentation of a card connecting to a virtual secure server for display of specific protected online content has wide application in video content distribution industry.

[00016] A QR code is a matrix code or two-dimensional bar code. From the design perspective, as an example of present disclosure, as shown in **Figure 2**, the dual QR code **110** system contains, on one panel, tagged information in encrypted data packets pointing to proprietary screen, and on another panel, an unencrypted QR code for advertisements/promotions and other publicly available content, in one embodiment.

[00017] The virtual server of the system of an embodiment is configured to receive packets of encoded QR codes **110** from one client per embodiment. It is configured to evaluate the QR code or QR code data from the client, and in response to transmit a respective feedback response for access by the client on their mobile device **420**, restricted by a time duration. The back-end system analyses the QR code data packets in order to identify the location of its storage on the virtual server and generates/formats the copyrighted encrypted content to be securely transmitted to the client’s device. The content is marked with a unique identifier (ID) based on the individualized licence key locked to the mobile device **420**. The ID allocation can be determined according to the specific application scenario.

[00018] More specifically, a browser running on the client's device will establish a coupling or connection to the mobile infrastructure (e.g., a W-CDMA, Transmission Control Protocol/Internet Protocol (TCP/IP) coupling or all other variations of wireless connection, now and in future). Information and messages are broken down into smaller pieces, or packets, to be transmitted from a source to a virtual destination. The protocol breaks down and reassembles the data packets, while ensuring the data packets are transmitted to the proper destination. Each data packet is given a header that contains a variety of information, including the order in which the data packet is to be reassembled with other packets for the same transmitted message or information. Each data packet is put into a separate IP envelope for transmission over the internet. The IP envelopes contain addressing information that direct the internet **610** to a destination address. All IP envelopes containing data packets for the same transmitted message or information have the same addressing information, in order that they are all transmitted to the same destination location, and thereafter, properly reassembled. Each IP envelope also contains a header that includes information of the source, like client's device ID, IP address, the destination cache, the amount of time the packet should be maintained before being discarded, etc.

[00019] This disclosure also covers various methods of invoking encrypted data packets using client's mobile devices **420** as part of the single integrated platform. Near field communication (NFC) or similar technologies can also be incorporated into the embodiment which will enable QR code access by merely placing the physical embodiment near the client's mobile device **420**. In such a circumstance, after client verification through their portable devices, encrypted data from QR codes **110** will automatically be streamed from a DRM enabled media server, decrypted and played by the trusted media player on the mobile web platform. Client must still pass through security authentication for all encrypted data packets. Encrypted data is strictly copyrighted DRM protected digital content only. This provides security and thwarts piracy of digital audio and video information that is streamed/locally downloaded from the internet or other suitable partner network.

[00020] No user interaction will be necessary to obtain digital streaming of unencrypted content which is hosted publicly on the internet. The unencrypted content may be for example, but is not limited to, audio and/or video media such as songs, movie scenes and promotion material, extra on-line services such as downloadable exclusive content, movie previews, lyrics, video clips, news relating to the digital content, access to chat and forum meetings, photo albums, special offers or any other suitable additional information that is available in public domain.

[00021] In another method, client can access information using their native QR code scanners built into their mobile devices **420** and such invoking method will require a two-step process of (1) point and (2) scan for both types of QR codes, encrypted and unencrypted.

[00022] Current mobile devices which scan the disclosed embodiment are pre-configured to transmit the scanned data through their native operating system software and this invention doesn't take any credit for that technology. However, in order to use the full feature of this proprietary content delivery integrated system, the client must be in possession of physical card and no remote device recognition for data transference is allowed or available. The QR codes strictly serve as a means to an end and store only one "individualized" (client specific), locked to their device, address to the URL, securely embedded within the system.

[00023] This disclosure also describes a unique process of "individualizing" mass QR codes to cater to individual client needs. This is achieved through a seven-step process as described next. A unique URL of proprietary online screen is obtained as step one. Secondly, using a URL shortener, this link is restricted. Then the shortened link is converted into a dynamic link using an SDK. Fourthly, multiple dynamic links for the same proprietary online screen are generated. In the fifth step, each link is assigned a different password. In the next step, additional security is selectively put like time duration of link availability. Lastly, these restricted, individualized are stored securely in a content database which will now have one link for every unique password pointing to the proprietary online screen. This process helps to "individualize" QR codes and forms the backbone of this invention. Individualizing where each client is pointed to such that it is restricted by a password and has an expiry date as controlled by the back-end system enables individual personalized delivery of key required for securely playing the content. It also offers higher levels of interactive with the end user.

[00024] In an embodiment of a QR code recognition activity for interactive entertainment, a client requests an XML (eXtensible Markup Language) file comprising a web page for use in a QR code function. The QR code function of an embodiment includes a QR code **110** processing exercise from the server supporting QR code recognition. The QR code function of an embodiment also includes use of the URL from the decoded QR code to return a secure web page for which authentication is required to the client. The proper XML file is returned to the client from the virtual server, via the internet or wireless network, and the client's browser displays the text, graphics and multimedia data of the file on the client's mobile device screen.

[00025] Methods and systems as described here are for using QR codes on physical tangible business card sized objects (paper, polymer, plastic or else) to launch an interactive mobile only

proprietary screen which when scanned with a client's mobile device **420** has an application to read QR codes or a QR code recognising inbuilt camera. The QR code **110** can be provided in the embodiment, e.g., but not limited to, label, tag, printed, imprinted, embossed, or moulded into product, sample, surface, label, or tag. The server of the system of an embodiment is configured to receive decoded QR code data or packets of encoded QR codes from *one and only one source*. The QR code recognition of an embodiment enables the provisioning of video content in real-time or near real-time via client's portable device coupled to a wireless network or internet **610**. The QR code embodiment acts as a tangible bridge providing online video access through an offline consumption method. The physical card is a standalone retail product available offline.

[00026] An embodiment of QR code recognition processing for interactive exchange begins when a user scans a QR code **110** using his/her client device. The QR code includes "personalized" secure data packets pointing to a secure virtual cloud portal. The client decoder sends the QR code data request to the server supporting the QR code processing application and the URL from the decoded QR code via the network.

[00027] Disclosed herein is a package for display and sale of a card product comprising of, as an example, a first panel connected to a second panel via a first fold line. The card region of the first panel is perforated such that the card can pop out to become a standalone product minus the packaging. The reverse side of the first panel is reserved for instructions, pricing and any disclaimers. The second panel is also perforated from the first panel along the fold line and contains printed information about the secure and DRM protected content that unique QR codes **110** (printed on the perforated card region) point to. The reverse side of the second panel is however left for sharing any other information, advertising, sales tracking universal barcodes or SKUs. It is another object to allow retailers to integrate additional promotions and information into a promotional or cross-promotional label of the invention even though the tag can be affixed by the manufacturer.

[00028] This description also covers all other variations of packaging possible, not included in this example. The number of folds can be increased or decreased based on requirements and should not be considered as a limitation.

[00029] This disclosure also covers methods for activation of the single integrated system on a card. The tagged card as described in this patent holds zero value until its activated. In contrast to credit and bank cards issued by financial institutions, the client account will be represented

by the “individualized” QR and a unique password **101**. Unlike gift cards, the card included in this embodiment cannot be activated by the retailer.

[00030] In accordance with the above, it is an object of the present invention to provide methods to make QR codes “interactive” through a simple, inexpensive or convenient enhancement such that there are opportunities to personalize communication with each client through the product described in this disclosure.

[00031] The tangible card in this embodiment requires a two-step process to activate. The media playing device (typically, but not limited to, a smartphone or tablet) has an inbuilt communication interface such as a network interface to allow it to communicate with one or more networks including for example, the internet or any other suitable networks like home wi-fi. The communication interface preferably provides secure communication with the remote device which contains the copyrighted digital content such as the media content server **620**.

[00032] Activation of the card starts a ticker in the back-end systems and limited access to secure content is provided to the consumer for a definite limited time period. Subsequent activity by a client using card is also tracked using the digital signature **501**. Upon authentication, the unique digital signature **501** interacts with the communication interface hosted virtually. This interaction is a function of content server **640**, digital rights management server **630** and media content server **620** whose processes are elaborated below as well. The result of the combined function results in the display of the content on the client’s device.

[00033] As shown in figure 3, the media content server **620** and the communication interface **520** may be coupled through any suitable links. The media playing device is also in operative communication with a digital rights management service provider which may be one or more servers for example. In addition, the media playing device is also in operative communication with a content service provider which may be for example another web server that provides other content other than the encrypted digital audio and/or video media content provided by the media content server **620**. For purposes of illustration, the media content server **620** will be described as a server or other network elements that provide encrypted media **712** such as encrypted audio and/or video media that is to be played by the media playing device.

[00034] **Figure 4** is a block diagram illustrating in more detail an example of a media content delivery system. As shown in this example, the controller **1000** includes an encrypted QR code **110** locked with a unique password **310** (as displayed on the physical embodiment) along with a “identified and locked” media playing device through a digital signature **501**, embedded

media player **711**, authenticator user interface **311**, web browser **211**, media cryptography engine **621**, control logic application **1000**, and real time streaming system **720**. The block is preferably software application in the form of executable instructions native to the media playing device that are stored in memory (not shown) such as RAM, ROM, distributed memory or any other suitable memory as known in the art. These software applications are preferably executed by a processing chip with access to central processing unit, or any suitable processing device or plurality of devices.

[00035] Also, the controller is interactively connected in real time to a time-based cryptography client application **511** and a looped counter based cryptography client **512**. The digital rights management service provider may likewise include a corresponding time-based cryptography server **633**. The time-based cryptography client **511** may, for example, provide another level of security between the digital rights management service provider **630** and the media player device **420**, by encrypting content identification information or any other suitable information. As used herein, encrypting also includes sending a representation of an ID from which the ID can be constructed from the representation. The time-based cryptography server **633** if employed receives the time based encrypted information and decrypts the information as necessary to determine the content ID, which also provides a level of authentication as known in the art.

[00036] The real time streaming system **720** includes the playing device identification data **715**, received media **714** as received from for example the digital rights management service provider **630** received encrypted keys **713** such as received decryption keys sent by the digital rights management service provider, and encrypted media **712** which is the media content obtained based on the content ID in the transmitted in the digital signature **501** (Password + Mobile device Id+ OTP). The real time streaming system **720** is preferably local for security reasons but may be remote if proper security is provided.

[00037] The digital rights management service provider **630** as previously noted may be one or more web accessible servers whose functionality may be distributed if desired or co-located in the media content server **620** or any other suitable location. In this example, the digital rights management service provider **630** includes content matcher secure weblink **631** through a content registry database **643** which includes stored content identification information (content ID) which identifies media and/or content to be streamed. A linked list of media IDs serves as part of a playlist (list of media files to be streamed) for the media player, in case of multiple registrations. The content identification information is linked with media identification information to designate a class, group or type of media/content to be streamed. The media

identification information contained within the content matcher weblink **631** also includes data representing, for example, media file name, the URL to access the corresponding encrypted media file for the right media type. As such, the content registry database **643** includes linked content identification information and media identification information. The content identification information may include, for example, content name and data representing a description of the content. The key database **644** may include, for example, the media identification data and its corresponding decryption key such as a triple DES encryption key(s), or any other suitable encryption key(s) and initialization vectors if necessary.

[00038] The digital rights management service provider **630**, in one example is a suitable server and may include one or more processors and associated memory or any other conventional structure to carry out the operations required by the content matcher weblink **631**. This application may be executable instructions stored in a memory (not shown) and executed by one or more processing devices of the digital rights management service provider. The media content server **620** includes media delivery secure weblink **622** and content management database **623**. The media delivery weblink **622** facilitates the streaming of media for example, in HTTP format through an embedded player, or any other suitable format through a suitable communication interface **1001**. The content management database **623** may include a user interface **210** that allows an operator to remove or add media in directories for streaming. For example, the content management database **623** may allow the deletion or addition of media, whether encrypted or unencrypted, to a suitable directory.

[00039] The content web application server **640** may be for example one or more servers that contain website information that are accessible via uniform resource locator information or any other suitable locator information as known in the art. It will also be recognized that the content web application server **640** and other servers may be a plurality of servers since content may be located on several different servers and accessible through any number of applications.

[00040] The control logic application **1000** controls all of the necessary components at any given time to communicate with for example the communication interface **1001** as well as other applications in order to provide the requisite output as described herein. The control logic application **1000** may also, for example, obtain the stored player ID **715** and send it through an appropriate secure layer communication link to the digital rights management service provider through the communication interface **1001**.

[00041] The arrows shown represent operations or communications between devices. These communications may occur over secure links using known protocols, and by way of example, will be described with reference to HTTP based protocols.

[00042] In addition, the DRM service provider **630** obtains data representing at least one cryptographic decryption key **603** which may be for example the decryption key itself or an index to another location to get the decryption key, or it may be for example a hash of the key, or any other suitable representation of the key for the encrypted content that is indexed by the content registry **643**. If the media playing device **420** includes a cache of previously obtained media files, the method includes checking the cache of previously obtained encrypted content using the received media ID from the playlist to see if the newly received content was retrieved during a previous session as is described in block **604**. However, if no cache is used, this step may be avoided. However, if a cache is used and if the encrypted content is not present in the cache, the playing device retrieves encrypted content from the media content source such as the media content server **624** using the media ID (namely the URL provided by the DRM service provider **630**). Hence, the encrypted media **712** information, such as the encrypted video and/or audio information that can be played by the media playing device is obtained.

[00043] If the cache is used, then the retrieved encrypted content is stored in the cache as shown for example in block **605**. As shown in block **604**, the method includes decrypting, such as by the media cryptography engine **621**, the encrypted media using the data representing at least one cryptographic decryption key so that the media player **420** can play the decrypted media file. This is shown for example by line connecting to block **420** in **figure 5**. If the DRM service provider **630** in addition to sending the URL for the encrypted media also sent for example a URL for additional content provided by the content registry database **643**, the method includes securely accessing an on-line service that is indexed by the media ID or that may be indexed by the decrypted media file if another media ID is present in the encrypted media file. This is shown in block **607**. This method includes playing the decrypted content that was obtained based on the “individualized” QR code **110** identification from the embodiment disclosed here by the media player **420**. The media content playing device **420** commences playing of retrieved additional information associated with the digital signature **501**, such as digital audio and/or video media content, in response to the retrieval of that information.

[00044] This information is returned in the form of a playlist of media URLs and media identifiers with corresponding keys and/or website URLs with appropriate credentials to allow the media playing device **420** to access the media content server **620** and for the media content server **620** to retrieve the appropriate encrypted media. This is shown for example by block **603**

and communication line leading to block **643**. The content registry database, in this example, also includes a content/media mapping table which for example may guide specific number of iterations (a closed loop) that are provided by content registry database **643** with encrypted media files so that when the encrypted media file is requested, additional information from the content registry database **643** relating to the encrypted media is also sent to the media playing device **420** allowing for delivery of encrypted data only a predefined number of times. The key database **644** is preferably linked with a content registry database **643** such that when the content ID is received, the content registry database **643** can also point to the appropriate decryption key for that given content. The DRM service provider **630** then securely sends the playlist for the media playing device **420**.

[00045] Figure 7 illustrates a block diagram of the digital rights management service provider which is a trusted authority, and therefore by way of example, may issue and/or sign digital certificates, or provide other suitable trust information as known for example in the public key/private key and symmetric key cryptography fields. The DRM service provider **630** may serve as the digital audio and/or video media encoder as shown in this example. As such, in this example, the content registry database **643** is populated with media identification, known as media ID and the key database **644** is populated with appropriate decryption keys for given media content and initialization vectors for each media identifier since one media server may store multiple media files and each media file may have a separate media identification or identifier. Also, media may be downloaded from multiple media content servers. The DRM service provider **630** also includes a content registry administration interface **646** that may be, for example, a graphic user interface **210** to allow an administrator to link database entries of target URLs with the corresponding media identifier.

[00046] In operation, an operator may enter a media name and an associated target URL of where this information is stored for entry in the content registry database **643** as media identification information. A media encoder **625** suitably encodes (encrypts) an imported media file from a suitable media file source and produces encrypted media content which is then stored in the media content server **620**. Any suitable encryption technique may be used such as triple DES or any other suitable encryption scheme. The DRM may publish the encrypted media a directory or other suitable storage location. The corresponding decryption keys are then stored in the key database **644** and indexed with the appropriate media identification information so that the appropriate decryption key is linked to the corresponding encrypted media.

[00047] In summary, media is effectively packaged by encrypting and registering the resulting media file with a unique media identifier. The media identifier contains the target URL of the

media file. The selection of the media may be performed through a suitable content registry administration interface. The encrypted media files may be published to a media service provider and randomly generated initialization vectors and decryption keys are stored in the DRM service provider **630** database.

[00048] The digital rights management service provider **630** is responsible for centrally and securely managing media identifiers (media ID), content identification information (content ID) and keys to encrypted media. The digital rights management service provider provides a secure web service frontend that is accessed by the media playing device to retrieve digital rights and pointers to media files and online services. It also provides administration tools that enable media management such as the encryption and publication of media files as well as content management. Such as the creation and control of content on the media objects.

[00049] It will be recognized that control information may also be embedded in the information sent back by the digital rights management service provider. For example, the order in which the media identification information is sent back may be dictate for example, the order in which the media playing device streams content. Alternatively, control information such as any suitable data, may be embedded in the communication which is then interpreted by the controller of the media playing device to play content in a certain order.

[00050] The controller is implemented by discrete logic through any suitable combination of hardware (mobile playing device), software (a combination of Google Widevine/ Apple fairplay/ Windows Playready), front and back end processing portal. Similarly, the digital audio and/or video playing subsystem may be implemented as one or more suitably programmed software players that carry out, as known in the art, MP4 (or other suitable extension) files for playback, or any other suitable audio or video stream playback. The controller, as described in this disclosure, also includes virtual cryptographic engines to facilitate authentication of the QR codes if desired and to decrypt retrieved encrypted media from, for example the media content server **620**. Once the encrypted media has been decrypted, it is then passed to the digital audio and/or video media playing subsystem to be played.

[00051] In another embodiment (as an extension to the current disclosure), the QR code **110** may include encrypted identification information by itself storing the password as data packets and hence eliminating the need for entering a separate “unique” password on each iteration of physical card usage. This changes the composition of the digital signature but keeps the backend systems, methods and processes identical. The QR code may also, in the future, include if desired, digital media container authentication information. The digital media container

authentication information may be any suitable electronic authentication information such as but not limited to a digital signature **501** of the trusted DRM service provider **630**, or other trusted authority that generated the authentication data for the “individualized” QR code. Alternatively, any other suitable mechanism may also be used for authenticating the digital signature, QR code or otherwise. In this example, the “individualized” QR code **110** information or any portion thereof is securely stored in tag memory and can only be read by a trusted QR readers. Providing authenticity allows for the DRM service provider **630** and/or other media content providers to trust the QR code enabled object (e.g. that it is not a pirated item). For example, only QR code objects with proper security functions can read the tag information. The tag contains remote content identification data may be for example stored digital content of any form, a location of where the media is ultimately stored, a network locator for a media server, or any other suitable content identification data that identifies in some manner, directly or indirectly, the content or media that is to be remotely pointed to by the QR code.

[00052] It will be recognized that the QR code **110**, if desired, may also be embedded in or otherwise coupled to the digital storage medium, itself as opposed to being placed on a card package or embedded with a container, in the future. As such a digital media storage in a chip card format which is considered as a digital storage medium may also have the QR code identification that can provide information about the data representing at least a digital media container authentication information, the encrypted QR code data and remote content identification data. Through these digital storage chip card, owners or users can securely obtain access to additional content or encrypted media by simply placing the container near or on the client’s portable mobile device. A high-level of security is provided and extra services and content can be accessed only when these encoded chip cards are physically present. Access codes cannot usually be simulated since the media data packets are encrypted on the QR code. Other advantages will be recognized by those having skill in the art. Any other suitable objects that employ an QR code that contains secure media data packets and remotely steamed/downloadable content identification information can be used.

[00053] As another example, this disclosure also covers multiple movies on the same card. In a single embodiment, multiple content can be presented in a sale to the client and its presentation can happen via a single digital signature **501**. As is presented in **figure 8, 9 and 10**, the system for multiple content – same form or different types (X, Y or Z), can be retrieved from the DRM service provider (as represented in **Fig 6**) after digital signature **501**, is confirmed via the portable device **420**. The respective content, X, Y, Z, in isolation or combination is sent by the

content service provider as Media_X 714_x, Media_Y 714_y or Media_{X+Y+Z} for its delivery on virtual media player 715.

[00054] It will be recognized that the order of the various steps described herein may be performed in any suitable order and that the above detailed description of the invention and the examples described therein have been presented for the purposes of illustration and description only and not limitation. It is therefore contemplated that the present invention covers any and all modifications, variations or equivalents that fall within the spirit and scope of the basic underlying principles disclosed above and claimed herein.

DETAILED DESCRIPTION OF THE INVENTION

[00055] Figure 1 is a flowchart illustrating one example of a method for securely obtaining video content to display using a retail card through offline online integration on a single platform.

[00056] Figure 2 shows a physical illustration of an example packaging of the retail card with a pop up option containing two panels. This illustration is symbolic only and actual shape of packaging can be different and this disclosure covers all known packaging styles.

[00057] Figure 3 is a block diagram illustrating one example of a digital media system in accordance with one embodiment to the invention. It lists the process of activating the retail card.

[00058] Figure 4 is a block diagram illustrating one example of a digital media system in accordance with one embodiment of the invention;

[00059] Figure 5 is a block diagram illustrating various communication sequences in a digital media system in accordance with one embodiment of the invention;

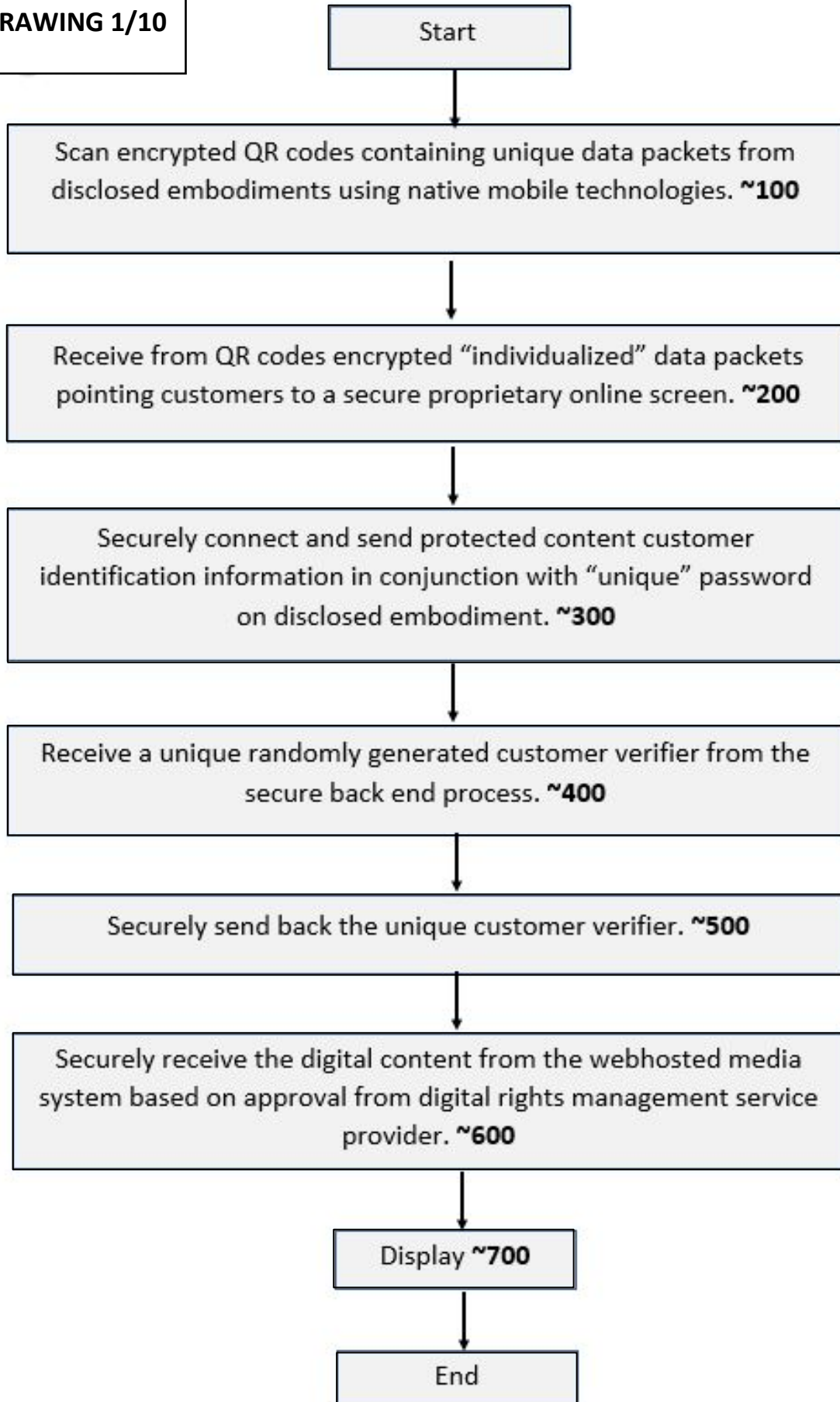
[00060] Figure 6 is a flowchart illustrating one example of a method of securely obtaining content from a content source in accordance with one embodiment to the invention;

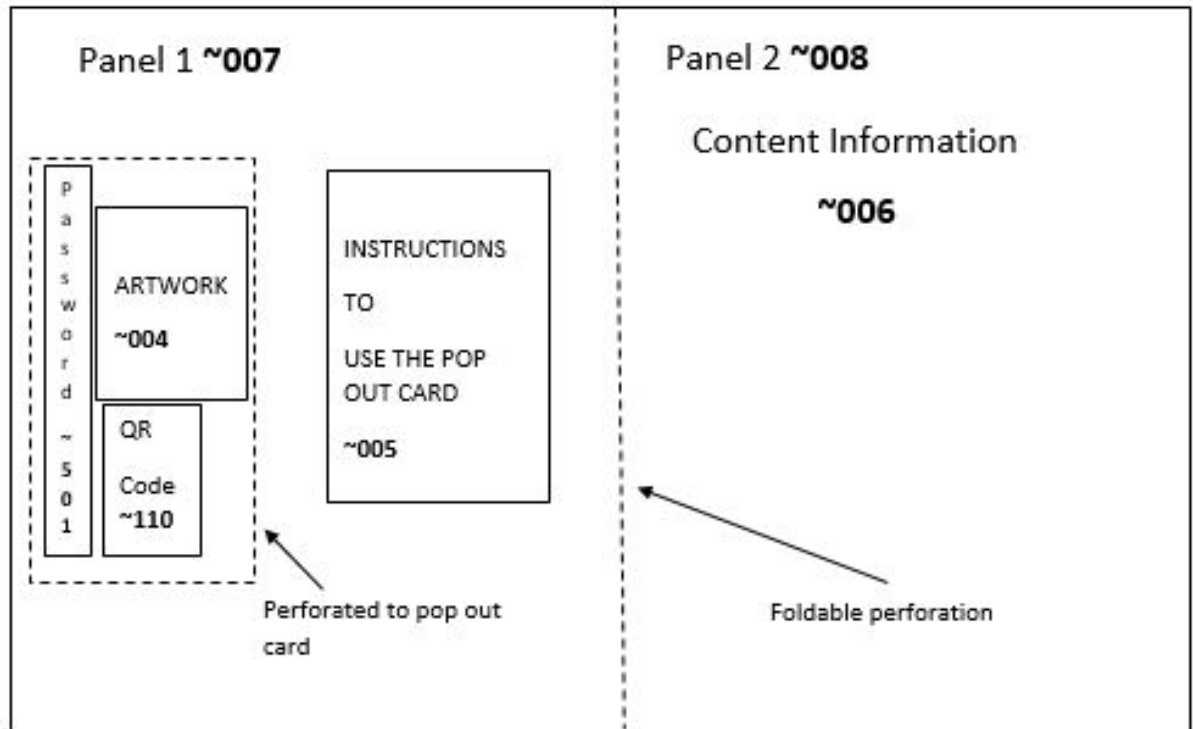
[00061] Figure 7 is a block diagram illustrating one example of a digital rights management service provider in accordance with one embodiment of the invention;

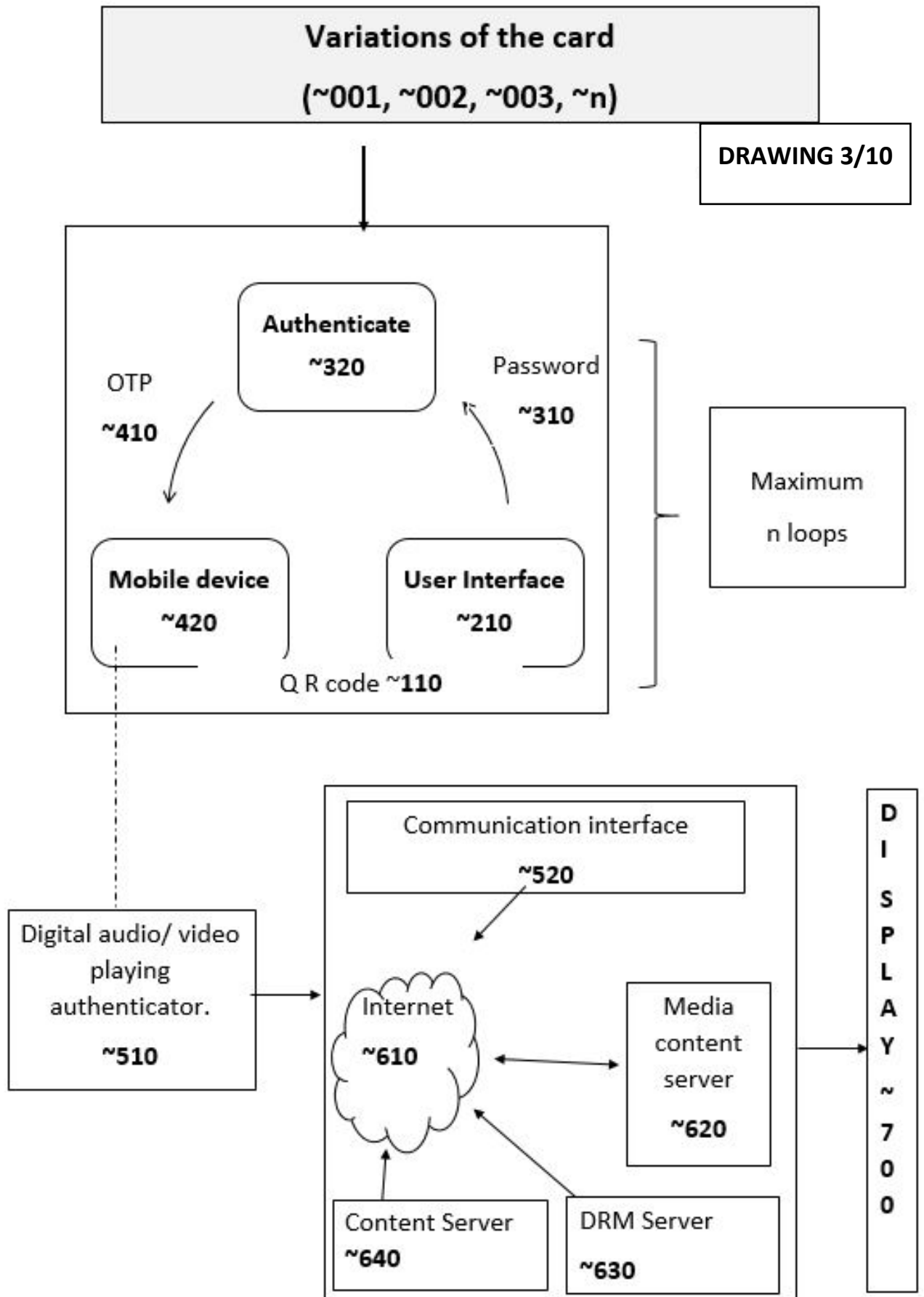
[00062] Figure 8 is a block diagram illustrating one example of a digital media X or content system in accordance with one embodiment of the invention;

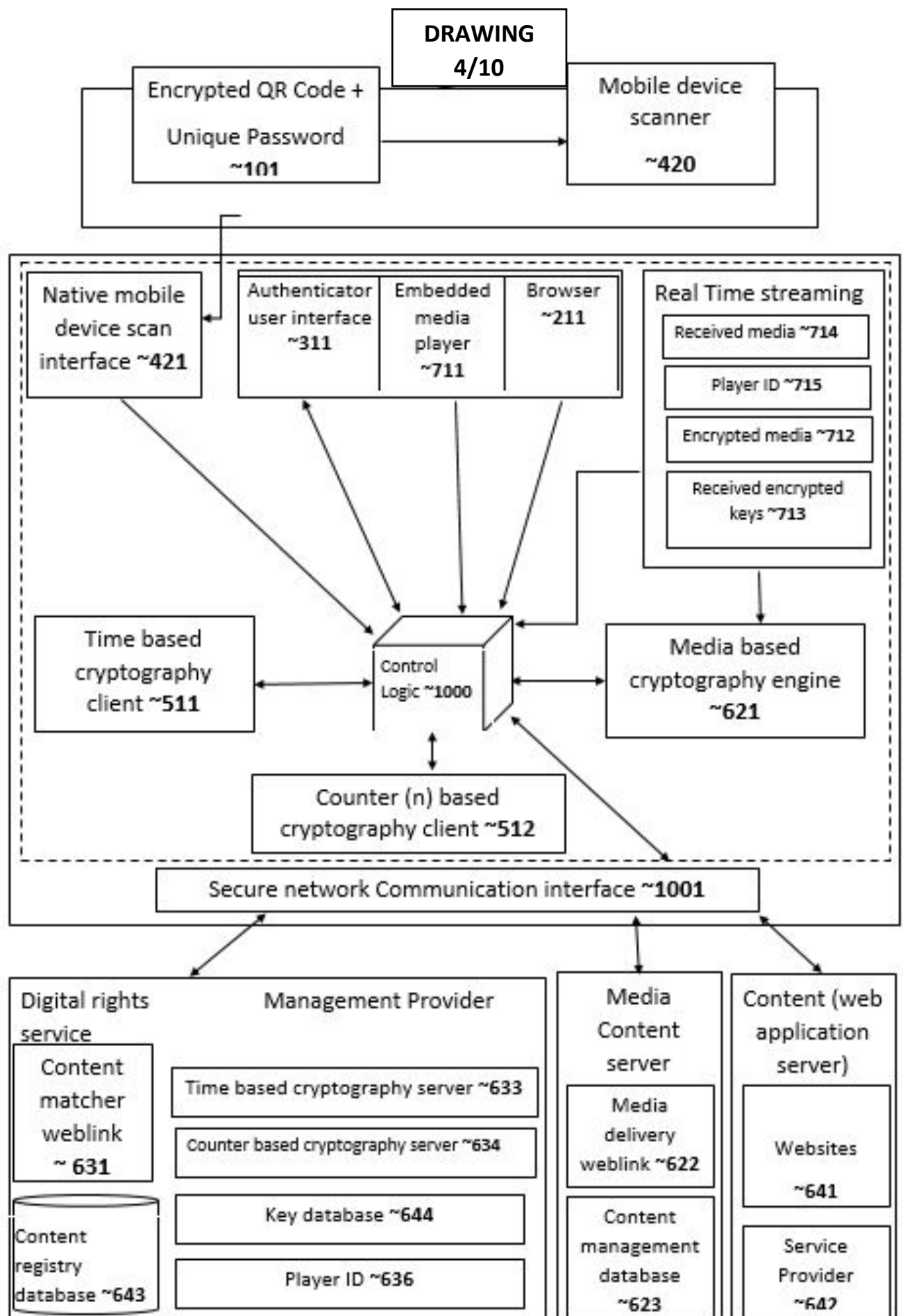
[00063] Figure 9 is a block diagram illustrating one example of a digital media Y or content system in accordance with one embodiment of the invention;

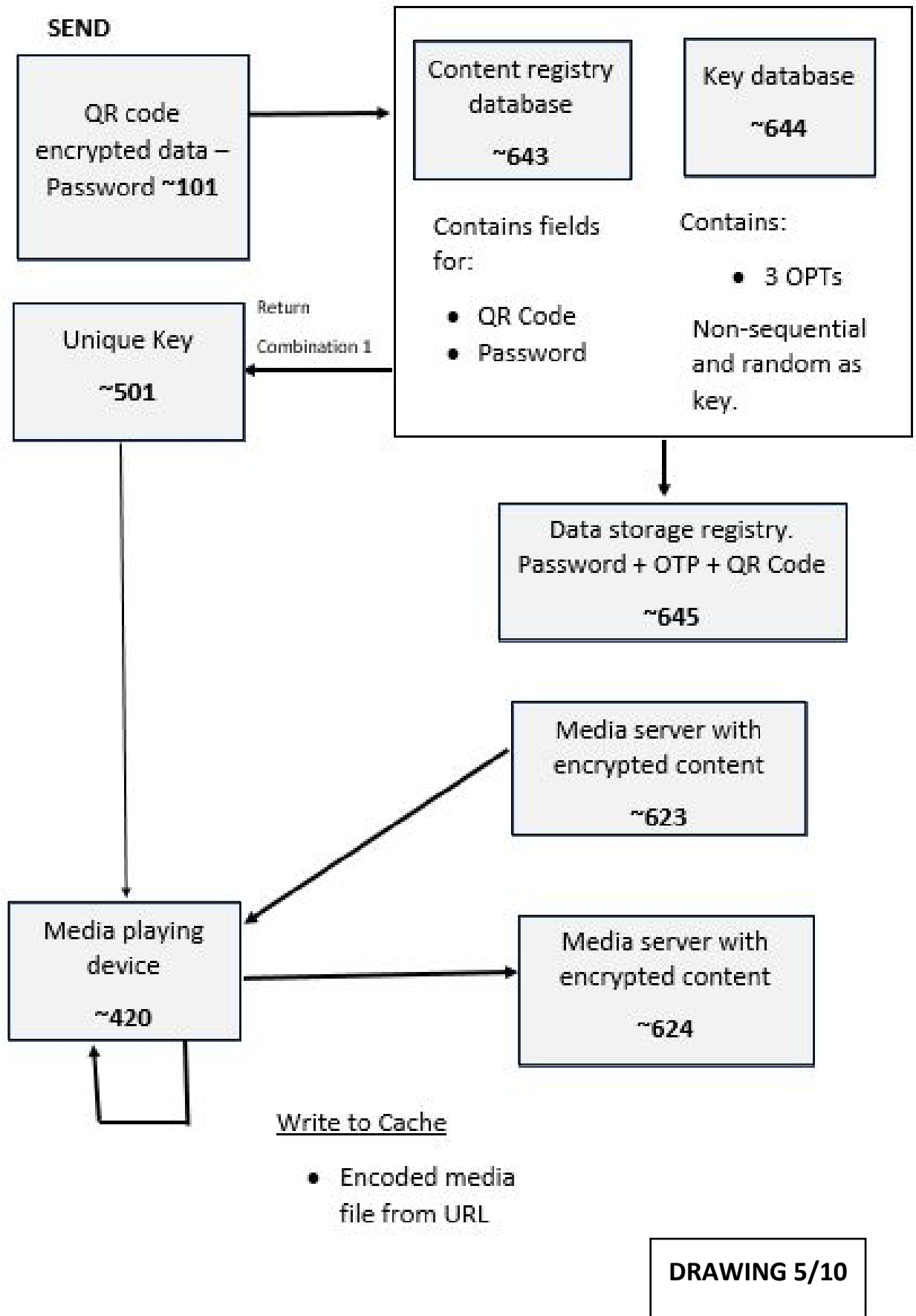
[00064] Figure 10 is a block diagram illustrating one example of a digital media X, media Y and media Z, combined together sent on a single digital signature accordance with one embodiment of the invention;

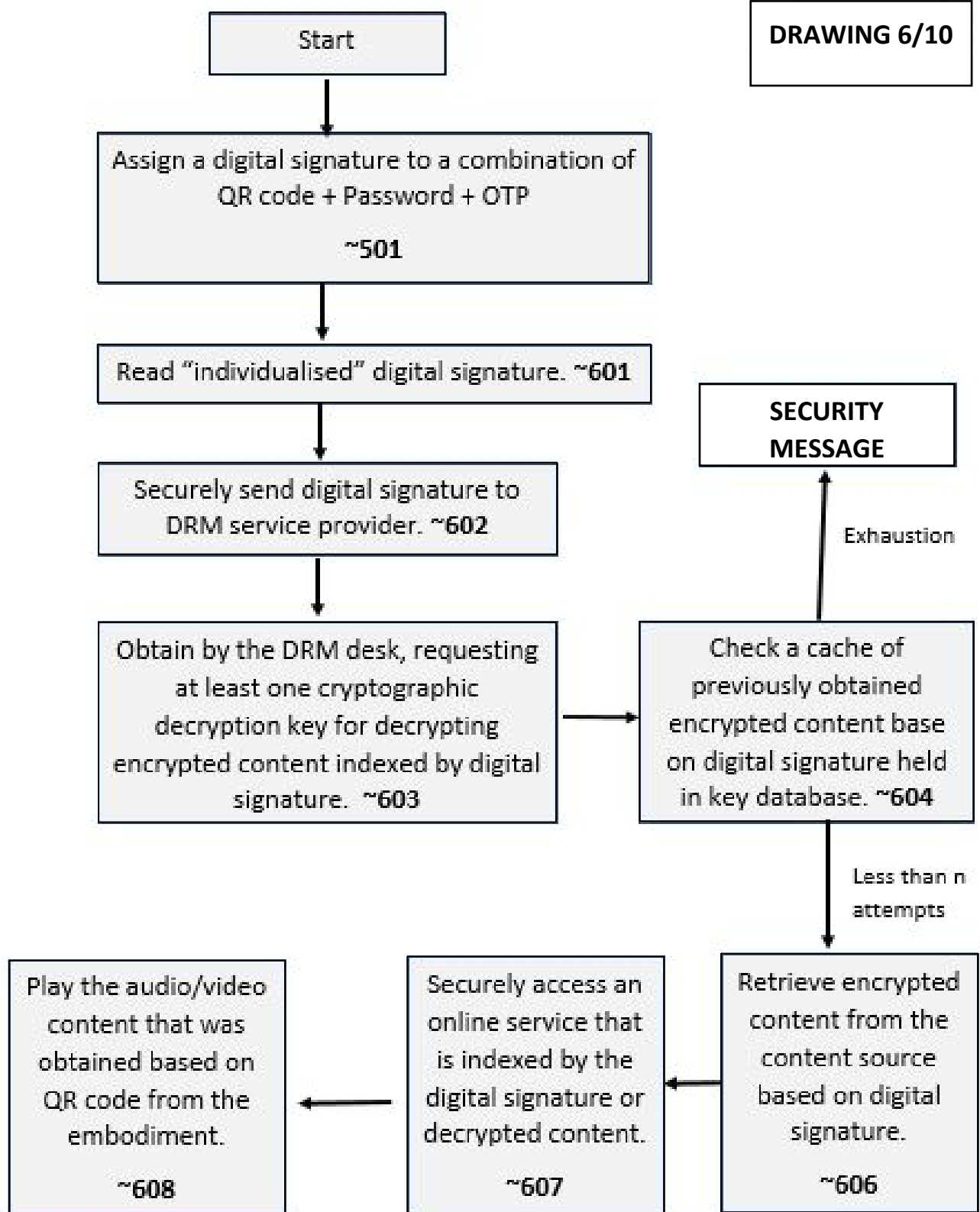
DRAWING 1/10

DRAWING 2/10



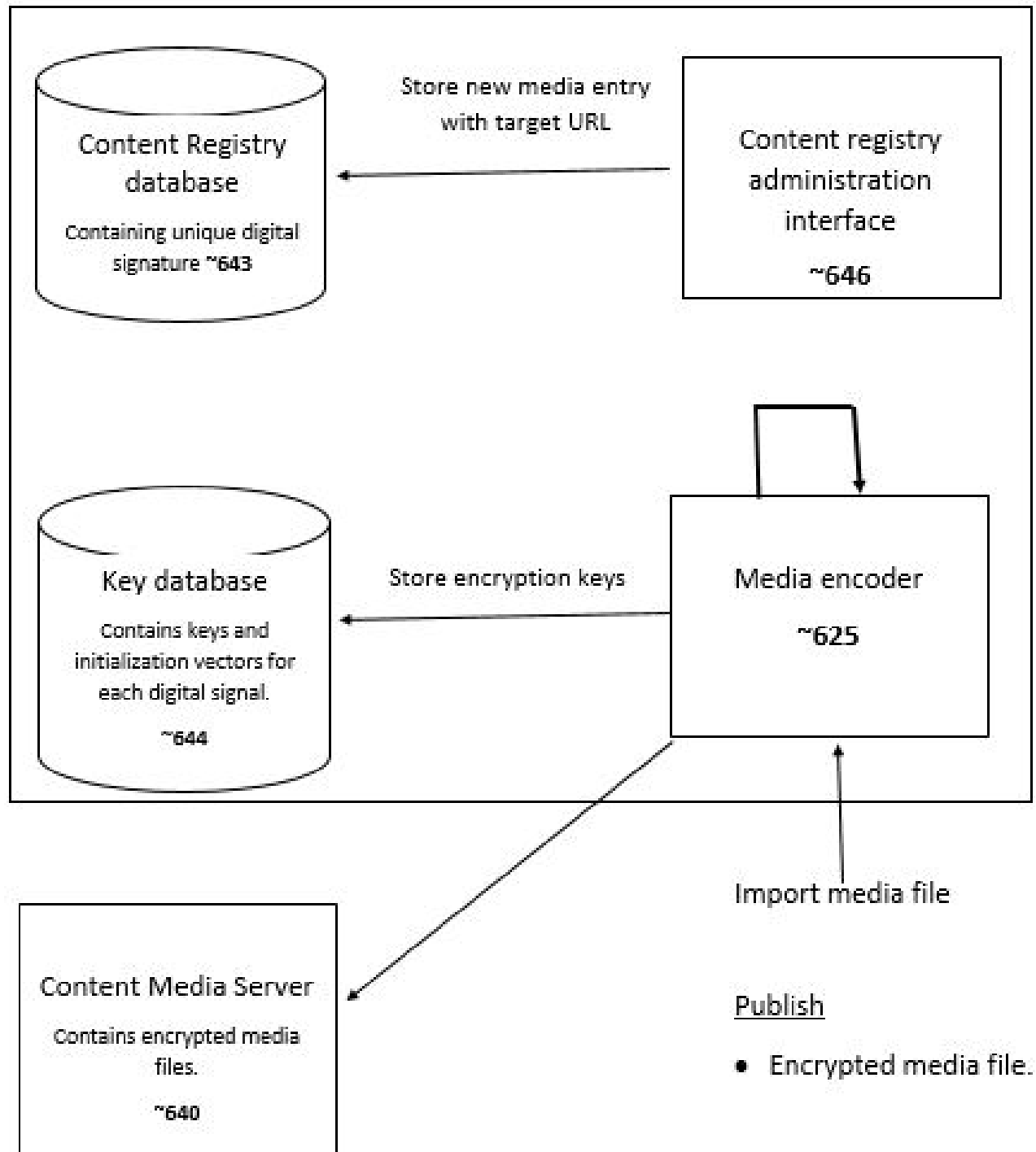




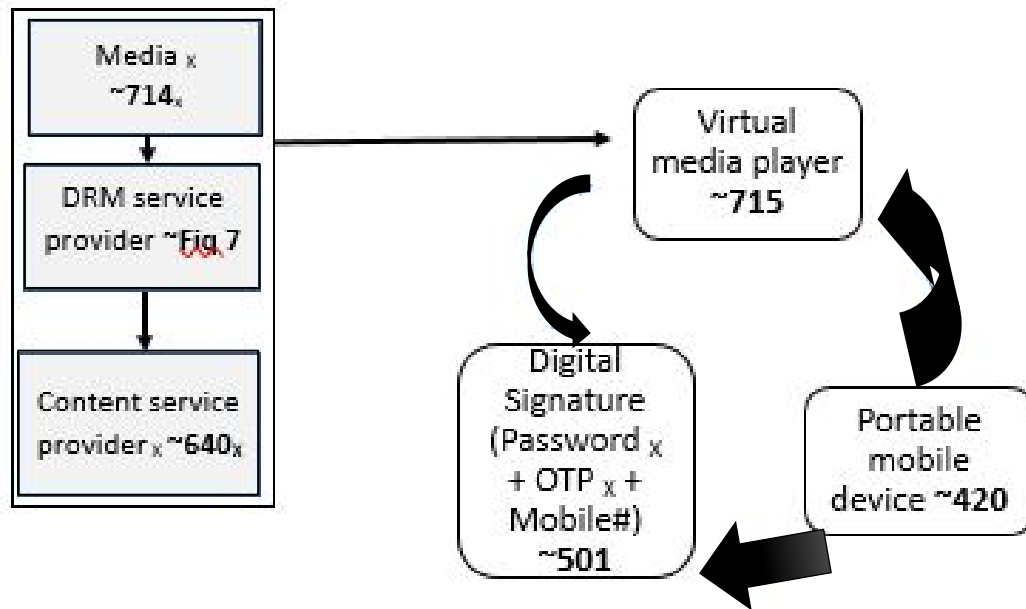


DRM service Provider

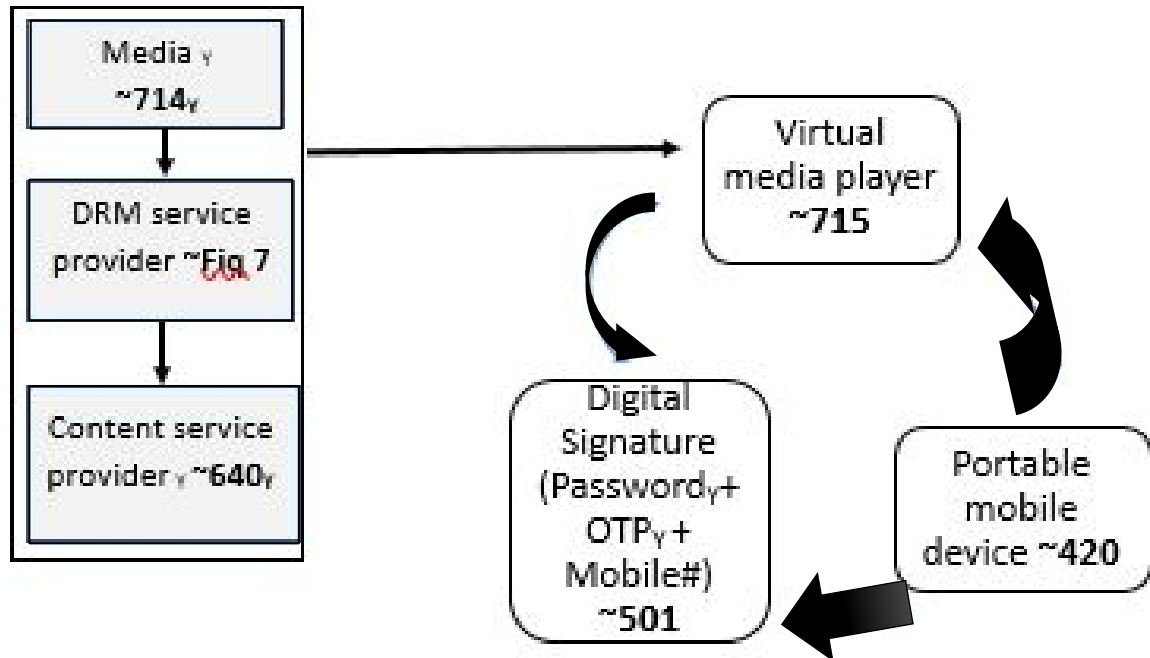
DRAWING 7/10



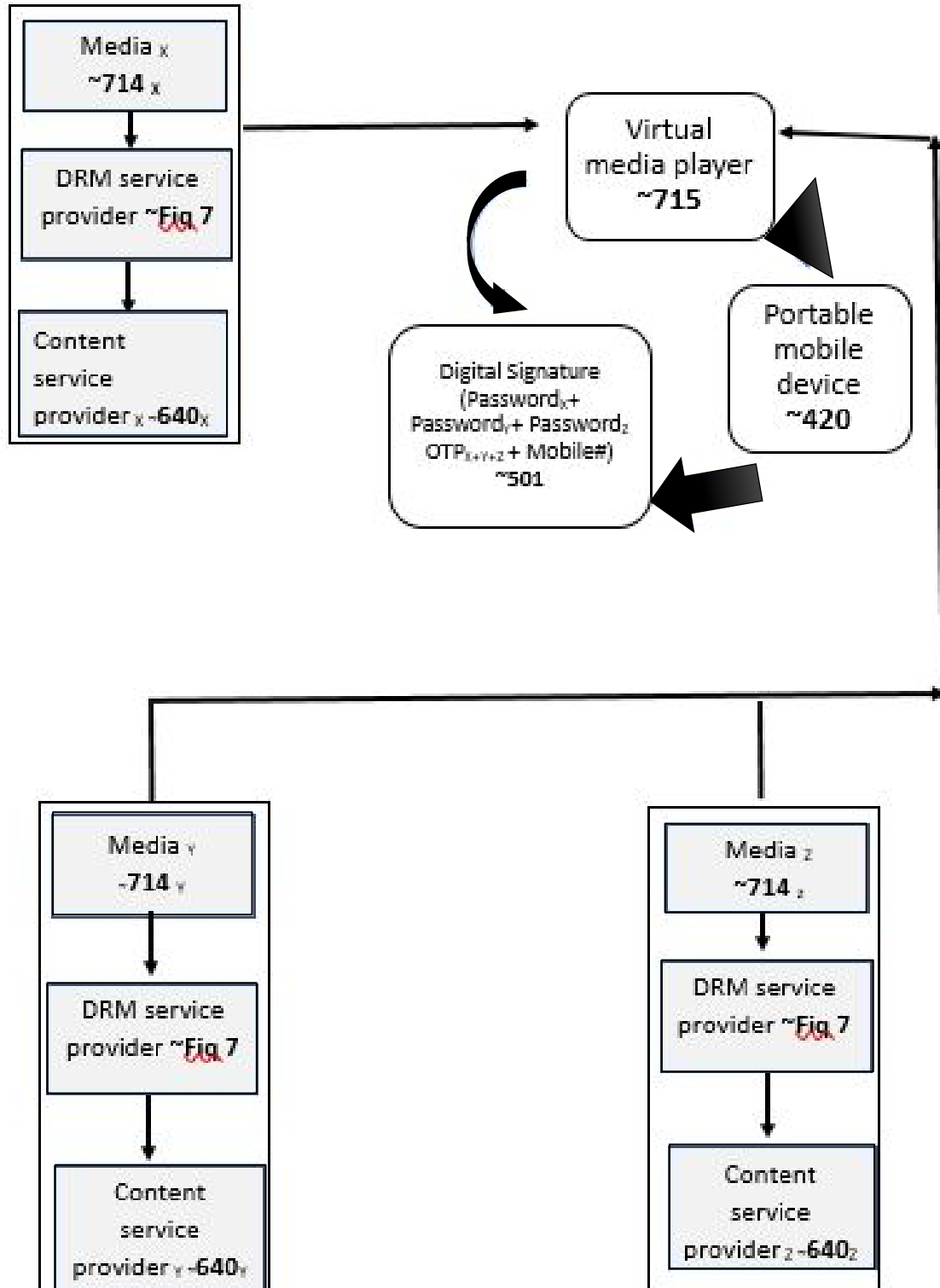
DRAWING 8/10



DRAWING 9/10



DRAWING 10/10



CLAIMS

This disclosure claims:

1. A physical tangible product comprising:
 - a digitally created interactive dual Quick Response (QR) codes;
 - pointing to a proprietary media content;
 - through a portable physical card;
 - scanned by a portable device with scanning inbuilt capability and transmitting at least one transmission packet;
 - packaging the physical tangible product transmitting the data packets from the printed/embedded QR code to the
 - its associated packaging of panels (of any material), one or plenty, in any dimension;
 - a virtual digital media container;
 - adapted to securely hold one or more digital content and
 - delivered through proprietary secure steaming or storage medium methods.
2. A method for individualization of URL QR codes comprising an intricate process:
 - a unique URL of proprietary online screen;
 - restricting this obtained URL through a URL shortener;
 - converting the shortened link into a dynamic link using an SDK creation of multiple unique dynamic links;
 - assigning a different password for each generated dynamic link;
 - addition of additional security like time based availability storage in a secure back end database.
3. A method for individualization of URL QR codes comprising of the following:

an embedded unique password into the QR code such that it doesn't require entering of the password for the user.

auto detection of QR code such that it leads to a unique online address, protected by a sequence of codes as that specific address is invisible to average user.

4. A method of auto-retrieval of online verification codes via:

application of sequenced flowchart comprising of unique digital signature, customer's unique mobile phone number and varied interaction with the browser on the smartphone.

autofill of the identified verification code into specific field on a proprietary unique one URL.

5. A method for mobile phones, tablets or other portable devices comprising:

secure access content;

a secure "individualized" QR code pointing to a proprietary unique one URL wherein that URL link generates a digital signature by a combination of printed password on claim 1, client's mobile number and randomly generated one-time password.

6. A combination of claim 4, further comprising:

security verification of the digital signature;

delivery of a single license key from the DRM content server and

display of content.

7. A method for securely obtaining content from a content source comprising:

receiving, from an internet/wireless network enabled object having content description thereon, secure, uniquely generated digital signature information and

content identification information relating to stream enabled content associated with the claim 1;

sending, if authentication was successful, the content identification information and

internet enabled media playing device identification information to a digital rights management service provider;

receiving, in response to sending the content identification information and client's specific media playing device identification information;

stream abled content identification information and at least one cryptographic key necessary to securely decrypt the content;

securely obtaining the content from the content source; and

decrypting the received content based on the cryptographic key.