DOCUMENT MADE AVAILABLE UNDER THE PATENT COOPERATION TREATY (PCT)

International application number: PCT/EP2013/051256
International filing date: 23 January 2013 (23.01.2013)
Document type: Certified copy of priority document
Document details: Country/Office: GB
Number: 1201063.3
Filing date: 23 January 2012 (23.01.2012)
Date of receipt at the International Bureau: 21 February 2013 (21.02.2013)
Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a),(b) or (b-bis)
Certified Office Copy

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with patent application GB1201063.3 filed on 23 January 2012, and as stored electronically on the Patents Electronic Case file System.

The Patents Electronic Case-file System is compliant with British Standard BS10008 - Evidential weight and legal admissibility of information stored electronically and ISO15801 - Electronic imaging – information stored electronically, recommendations for trustworthiness and reliability.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 28 January 2013
Patents Form 1
Patents Act 1977 (Rule 12)

Request for grant of a patent

**Application number** GB 1201063.3

1. Your reference P36649GB

2. Full name, address and postcode of the applicant or of each applicant

   YouView TV Ltd
   B6 Ground Floor, Broadcast Centre
   201 Wood Lane
   London W12 7TP
   United Kingdom

   Patents ADP number (if you know it) 10361947001

3. Title of the invention
   **Authorisation system**

4. Name of your agent (if you have one)
   "Address for service" to which all correspondence should be sent. This may be in the European Economic area or Channel Islands (see warning note below) (including the postcode)

   Mathys & Squire LLP
   Reddie & Grose LLP
   120 Holborn
   London EC1N 2SQ
   Greater London
   United Kingdom

   Patents ADP number (if you know it) 09752627001

5. Priority declaration: Are you claiming priority from one or more earlier-filed patent applications? If so, please give details of the application(s)

<table>
<thead>
<tr>
<th>Country</th>
<th>Application number</th>
<th>Date of filing</th>
<th>Date available on PDAS</th>
</tr>
</thead>
</table>

6. Divisionals etc: Is this application a divisional application, or being made following resolution of an entitlement dispute about an earlier application. If so, please give the application number and filing date of the earlier application

<table>
<thead>
<tr>
<th>Number of earlier UK application</th>
<th>Date of filing (day / month / year)</th>
</tr>
</thead>
</table>

7. Inventorship: (Inventors must be individuals not companies)

   Are all the applicants named above also inventors? No

8. Are you paying the application fee with this form? No

9. Accompanying documents: please enter the number of pages of each item accompanying this form.

   Continuation sheets of this form

   Description: 14
   Claim(s): 6
   Abstract: n/a
   Drawing(s): 6

If you are not filing a description, please give details of the previous application you are going to rely upon

<table>
<thead>
<tr>
<th>Country</th>
<th>Application number</th>
<th>Date of filing</th>
<th>Date available on PDAS</th>
</tr>
</thead>
</table>

(REV DEC07)

Intellectual Property Office is an operating name of the Patent Office
10. If you are also filing any of the following, state how many against each item.

Priority documents: 0

Statement of inventorship and right to grant of a patent
(Patents Form 7): 0

Request for search (Patents Form 9A): 0

Request for a substantive examination (Patents Form 10): 0

Any other documents (please specify): Copy of cross referenced document

11. I/We request the grant of a patent on the basis of this application.

Signature: Subject: GB, Mathys & Squire LLP, D. Kramer 20244; Issuer: , European Patent Office, European Patent Office CA

Date: 23 Jan 2012

12. Name, e-mail address, telephone, fax and/or mobile number, if any, of a contact point for the applicant

KRAMER, Mr. Dani
Email: mail@mathys-squire.com
Telephone: +44 (0)20 7830 0000
Fax: +44 (0)20 7830 0001

Warning
After an application for a patent has been filed, the Comptroller will consider whether publication or communication of the invention should be prohibited or restricted under section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you are resident in the United Kingdom and your application contains information which relates to military technology, or would be prejudicial to national security or the safety of the public, section 23 of the Patents Act 1977 prohibits you from applying for a patent abroad without first getting written permission from the Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked. Until such time or until the revocation of any direction, for any such application the address for service referred to at part 4 above must be in the United Kingdom.

Although you may have an address for service in the Channel Islands, any agent instructed to act for you must reside or have a place of business in the European Economic Area or Isle of Man.
Authorisation system

The present invention relates to an authorisation system, specifically an authorisation system for use in a content provision system. This invention also relates to a method of authorisation and to a receiver/decoder.

In the field of electronic data transfer, there has been much research in the security and reliability of the transmission of data. It is an intrinsic (and useful) property of electronic data that it can be copied and retransmitted. Many methods have been devised to overcome the negative aspects of this property.

The present invention relates primarily to the situation where the data is in the form of audio/video (A/V) content. In this case, the security of the data is important as charges and subscriptions may apply to certain content, and content providers may wish to retain control over their content and/or ensure that their content is only being sent to an authorised user, or to a device that has been authorised.

There are a multitude of content providers who use various delivery methods to transfer data, such as Digital Terrestrial Television (DTT), Internet Protocol Television (IPTV) and Video On Demand (VOD). Each has their own set of requirements when authorising a user, and different requirements on the use of data. For example VOD may have a time limit relating to when it can be viewed, and it may not be possible to record IPTV. This creates a complex network of trust 'pairings' between user devices and service or content providers.

In audio/video broadcasting and content provision systems, it is desirable to authenticate both users of the system and the system itself to users. In one example of a prior art authorisation system, each separate content receiving device (e.g. set-top box) produced by a different manufacturer has an independent trust relationship with each available content provider.

In order for an effective and efficient content provision system to operate, content providers ideally have a trust relationship with the consumer devices and vice versa. This is so that the content providers know that the device they are supplying content to is an authorised device which, for example, has the requisite subscription or Digital Rights Management (DRM) software. This trust relationship must also work in the
reverse; the consumer device ideally is able to trust that data it receives comes from an authorised provider, to reduce the chances of malicious software being downloaded, for example. A current solution is for each content provider to have an individual trust relationship with each device (and hence user). This becomes inefficient when there are a large number of content providers and/or users. The present invention aims to alleviate at least some of these problems.

Broadly, according to the present invention there is provided a system and method adapted for implementing an authorisation system so that a multitude of consumers or consumer devices can receive data from a multitude of content providers in a secure and efficient way via a trust authority.

The system and method are adapted so that content providers and consumer devices can be independently authorised as part of an ecosystem wherein consumer devices and content providers can mutually recognise one-another as authorised parties within the ecosystem.

According to one aspect of the invention, there is provided a method of authorising multiple user devices and multiple content providers in a content provision system, the method comprising: providing each content provider with a content provider authorisation certificate; providing each user device with a user device authorisation certificate, wherein the content provider authorisation certificate and the user device authorisation certificate originate from a common source; and determining whether each content provider and each user device is authorised to participate in the content provision system via a mutual exchange and comparison of said certificates between respective content providers and user devices.

The term "receiver/decoder" as used herein may connote a receiver for receiving either encoded or non-encoded signals, for example, television and/or radio signals, which may be broadcast, streamed, downloaded or transmitted by some other means. The term may also connote a decoder for decoding received signals. Embodiments of such receiver/decoders may include a decoder integral with the receiver for decoding the received signals, for example, in a "set-top box", such a decoder functioning in combination with a physically separate receiver, or such a decoder including additional functions, such as a web browser, a video recorder, or a television.
It is envisaged that the system as herein described may be implemented wholly on a central server, or a set of interconnected servers, which is/are connectable to a plurality of remote client devices. Alternatively, aspects of the system may be implemented, at least in part, on the or each (remote) client / user device.

It is envisaged that aspects of the system, user device and/or method described herein may be implemented in software running on a computer such as a personal computer or a receiver/decoder (which may be connected directly to a monitor or to a television or other display means), and it is to be appreciated that inventive aspects may therefore reside in the software running on such devices.

Other aspects of this system, user device and/or method may be implemented in software running on various interconnected servers, and it is to be appreciated that inventive aspects may therefore reside in the software running on such servers.

The invention also extends to a server or a plurality of interconnected servers running software adapted to implement the system or method as herein described.

The invention extends to any novel aspects or features described and/or illustrated herein.

Further features of the invention are characterised by the independent and dependent claims.

The invention extends to methods and/or apparatus substantially as herein described with reference to the accompanying drawings.

The invention also provides a computer program and a computer program product for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein, and a computer readable medium having stored thereon a program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein.

The invention also provides a signal embodying a computer program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein, a method of transmitting such a signal, and a computer
product having an operating system which supports a computer program for carrying out any of the methods described herein and/or for embodying any of the apparatus features described herein.

5 Any apparatus feature as described herein may also be provided as a method feature, and vice versa. As used herein, means plus function features may be expressed alternatively in terms of their corresponding structure, such as a suitably programmed processor and associated memory.

10 Any feature in one aspect of the invention may be applied to other aspects of the invention, in any appropriate combination. In particular, method aspects may be applied to apparatus aspects, and vice versa. Furthermore, any, some and/or all features in one aspect can be applied to any, some and/or all features in any other aspect, in any appropriate combination.

15 It should also be appreciated that particular combinations of the various features described and defined in any aspects of the invention can be implemented and/or supplied and/or used independently.

20 Furthermore, features implemented in hardware may generally be implemented in software, and vice versa. Any reference to software and hardware features herein should be construed accordingly.

Further aspects and/or advantages of the invention include:

25

- A system adapted to enable a content provider to trust a device, and a device to trust a content provider, without having individual trust relationships, including utilising a public key infrastructure for this purpose.

- Two-way trust, content providers trust devices, devices trust content providers.

30

- Means of ensuring a device (and hence user) has the requisite certificates for the required content and providing the content in a secure and non-transferable way.

- Putting a key onto a device, where the key may be known or unknown to the Original Equipment Manufacturer (OEM). This key is only accessible by the device’s System On Chip (SoC).

35

- A central authority overlooking trust relationships.
• The use of Public Key Infrastructure (PKI) – with a secure (Master) key associated with the device.
• Each device having a unique identity for content protection and to assist with management and monitoring.
• Keys provisioned to the device being renewable/revocable.
• The Master Key (MK) on the device is not accessible by software on the device other than via the SoC’s secure processor.
• The Master Key may be derived from a secret that is permanently bound in the SoC.
• If the MK is an unknown key, an alternative key is used to provision keys.
• The Master Key is rooted in, and bound to, the SoC.
• At least two ‘levels’ of keys: (i) a MK – nothing can change this, secure to device; and (ii) an Operational Key (OK) – used for day to day operations, and which is renewable/revocable.
• The manner in which the key is derived is implementation dependent and may use key ladders.
• The keys may take the form of asymmetric private keys with associated public key certificates.
• The device stores the public key certificate that corresponds to each of the private keys held securely by the device. In contrast to the certificates that are used as trust anchors, these certificates do not need to be held securely.
• In addition to the trust anchors, the device handles public key certificates that accompany documents and/or data protected by private key signatures to assert the authority of such signatures.
• A most trusted authority, which technically manifests itself as a self signed X.509 certificate.
• The device has the capability to securely manage confidential key material.
• The device prevents manipulation of the flash memory buses, or is robust against such manipulation. This is typically achieved by loading code into Synchronous Dynamic Random Access Memory (SDRAM) before verification and execution, or by physical means.
• The device protects against the alteration or replacement of all boot loaders, the Linux kernel, the Linux root filesystem and all other file systems within the device from which code may execute or trust anchors are stored.
• The device verifies the platform software on each boot.
• Subsequent levels of a boot up can be verified through signatures using keys
assured in earlier levels.

Further information may be found in the following documents, which are hereby incorporated in their entirety by reference:


Furthermore, reference is made to UK patent application number GB1020290.1, in the name of YouView TV Ltd, which is hereby incorporated in its entirety by reference.

The invention is now described, purely by way of example, with reference to the accompanying figures, in which:

Figure 1 shows a schematic overview of an authorisation system;

Figure 2 shows a more detailed schematic diagram of a portion of the authorisation system of Figure 1;

Figure 3 shows an example of the authorisation system of Figure 2 in use;

Figure 4 shows a diagram of the processing steps undertaken by the system of Figure 2 in operation;

Figure 5 shows details of the ways in which keys are stored and used in a user device of the system of Figure 2; and

Figure 6 shows an example of a Trust Hierarchy.

**Overview**

Figure 1 shows a schematic overview of an authorisation system 10 for a content provision system. The authorisation system 10 includes a Trust Authority / System Operator 226 which is adapted to vet and authorise a plurality of user devices 56, each optionally being provided by a different manufacturer, as well as a plurality of
independent and/or separate content providers 52, each adapted to provide data content items to users, via said user devices 56. The trust authority / system operator 226 is also referred to herein as a most trusted authority, or root certificate authority, depending on the context.

The content provision system is used to provide users with content, typically in the form of audio/video media content, such as broadcast content. In this case, the user devices 56 are in the form of set-top boxes (STBs), or the like, connectable to displays such as visual display units (VDUs), televisions or monitors.

The authorisation system 10 uses Public Key Infrastructure (PKI) involving the use of public and private keys and certificates to implement a trust model between the system operator 226, the plurality of user devices 56, and each of the content providers 52 thereby to ensure that all the entities in the system 10 are authenticated and appropriately authorised.

The System Operator 226 acts as a root certification authority, issuing and checking certificates of the other entities in the system 10 (as discussed in more detail below).

The system operator 226 hence determines which user devices 56 and content providers 52 are authorised to form part of the system 10.

This authentication system 10 results in a ‘horizontal’ model of trust in which numerous device manufacturers can use the same trust model to enable their devices to receive data from multiple different content providers. This is as opposed to a ‘vertical’ model in which different manufacturers must each have separate trust relationships with each content provider.

In this way, the number of required trust ‘pairings’ 222 (see Figure 1) between a number p of content providers 52 and a number m of devices 56 is reduced from an expected p x m to a more efficient p + m. The efficiency gains become increasingly large the larger p and m become. This system 10 is also much easier to add to or modify at a later stage. For example, were another content provider 52 to wish to join the system, only one additional trust arrangement 222 would need to be made; previously, without the use of Trust Authority 226, a new trust arrangement 222 would need to be set up for each device 56, which could become onerous.
As shown in Figures 2 and 3, the system operator 226 authorises content providers 52 and devices 56 in the following way. The system operator 226 provides a public root certificate TA1 100 (a “trust root”) to both the devices 56 and the content providers 52. The provision of TA1 100 to the device 56 enables the device 56 to validate a C5 certificate 120 that will be presented to the device 56 along with a specific software application (app) 302 signed using that C5 certificate. This application is a software plug-in provided by each content provider 52 and enables the device 56 to access data content provided by the content provider 52, or facilitate other services provided by the content provider 52. The C5 certificate 120 can be recognised as originating from the system operator 226 as it is derived from or rooted in TA1 100 (see Figure 2). TA1 100 is a self-signed certificate typically based on the X.509 standard.

The applications 302 are authorised either directly by the system operator 226, or by the content provider 52 with consent from the system operator 226. Thus, the device 56 can recognise the application 302 as authentic and trust the application 302 to obtain content from an authorised content provider 52. The reverse is also true, the content provider 52 can see that the device 56 is authorised to use the application 302 to access content (as explained in further detail below).

As shown in Figure 2, the system operator 226 issues an operational public key certificate 108 (e.g. OK2) to a device 56 which wishes to be authenticated. This may follow a step in which the device 56 requesting to be authenticated transmits a public portion of a cryptographic OK2 key pair it possesses to the system operator 226. In this case the system operator 226 signs the public portion of OK2 and issues the device 56 with a corresponding OK2 certificate 108. The provision of this public key certificate may occur via an intermediate certificate authority 102. OK2 108 is rooted in, or derived from, the trust root TA1 100 and can be recognised as such by any entity with knowledge of TA1 100. Thus, a content provider 52 can recognise authorised devices 56 by comparing the OK2 certificate 108 with the TA1 100 certificate held by the content provider 52.

As mentioned above, each content provider 52 provides an application 302 to a user device 56 to enable it to communicate and/or interact with the content provider 52, and hence receive content items and/or services from the content provider 52. Device 56 and content provider 52 communicate using this application 302. Each application 302
is associated with a particular content provider 52. Applications 302 are used so that each content provider 52 can implement their own method of communicating with a device 56.

5 Each application 302 is also authenticated or authorised so that the devices 56 know that the content they receive via the application 302 is from an authorised content provider 52. These applications 302 are authorised by being signed using the C5 “app signing” certificate 120, which is issued by the system operator 226, or by an intermediate entity 106. The C5 certificate 120 is also rooted in TA1 100 so that other entities in the system 10 can confirm the authenticity of the application 302. The process of actually signing the applications 302 with the C5 certificate 120 may be handled by either the content providers 52 themselves, or by the system operator 226. The C5 certificate 120 may then be provided by the content provider 52 along with, or bundled to, the application 302. The issuance of the C5 certificate 120 to the content provider 52 effectively constitutes the authorisation of the content provider 52. The C5 certificate 120 may be based on a C5 public key - forming one half of an asymmetric public/private key pair - originally held by the content provider 52, which is provided by the content provider 52 to the system operator 226 for signing by the system operator 226.

20 Once the above authentication steps have been completed, the system 10 comprises a trusted content provider 52 with a signed application 302 and a trusted device 56 with an operational public key certificate OK2 108. The application 302 is then passed to the device 56, either directly by the system operator, the content provider 52, or by other means. Typically, when a user device is switched on, applications 302 corresponding to content providers 52 which have been recently authorised by the system operator 226 are downloaded onto the user device 56 so that the user can access content from new content providers 52 using these new applications 302. This process occurs repeatedly so that the device 56 possesses an application 302 for each content provider 52 it has access to.

30 Once the above steps have been completed, the system operator 226 no-longer needs to be directly involved in the subsequent communication between user device 56 and content provider 52. The system operator 226 also has no direct role in the transfer of content 76. After the devices 56 and content providers 52 have been authorised or authenticated, the system operator 226 effectively 'steps out'.

When the device 56 requests content from a certain content provider 52, the relevant application 302 is executed. The application 302 communicates with the content provider 52, passing the public key certificate OK2 108 to the content provider 52. The content provider 52 can then check whether the user device 56 is authorised by checking OK2 108 against TA1 100. The device 56 carries out a similar procedure to authenticate the application 302 by checking C5 120, which was used to sign the application 302, against TA1 100. Once these steps have been completed successfully, the device 56 trusts the content provider 52 and the content provider 52 trusts the device 56. The requested content can then be passed from the content provider 52 to the device 56 using a suitable communication, encoding and encryption means.

The certificates OK2 108 and C5 120 are revocable. This is so that if a device’s subscription has expired, for example, it is no longer able to receive certain content. This could be achieved by adding a time limit to the certificate, or a certificate revocation list (CRL) being accessible so that devices 56 and content providers 52 can check if the certificates are still valid.

Figure 3 shows the system described above in use. The system operator 226 authorises the content providers 52 by issuing the C5 certificates 120. The application 302 provided by a content provider 52 is then signed using the C5 certificate 120, either by the content provider 52 itself, or by the system operator 226. The system operator 226 also provides content providers 52 with TA1 100. The system operator 226 authorises the device 56 by issuing OK2 108. The device 56 is also provided with TA1 100. As mentioned above, the applications 302 corresponding to each content provider 52 enable direct communication between each device 56 (one of which is shown in Figure 3) and each content provider 52. The device 56 is shown to have other embedded software such as Digital Rights Management (DRM) software 402 and a key box 400 where private keys may be stored. Once the content providers 52, applications 302 and device 56 have received their certificates, as described above, content 76 can be transferred directly between them. This occurs directly between the content provider 52 and the device 56 using the corresponding application 302.

Figure 4 shows a process undertaken by the various elements of the system 10 in use. Typically, there are of course numerous content providers 52 and user devices 56, only one of each is shown for clarity.
The process begins with the system operator 226 providing a public key certificate TA1 100 to a content provider 52 in step S1. TA1 100 is the trust root, or alternatively a certificate derived from, or rooted in, TA1 100. This process may occur via an intermediate entity 106 as shown in Figure 2. This public root certificate TA1 100 allows the content provider 52 to check whether or not particular user devices 56 are authorised.

The system operator 226 then authorises a user device 56 in step S2. The system operator 226 provides a public key certificate OK2 108, which is rooted in TA1 100, to the user device 56 along with TA1 100. Again, this may occur via an intermediate entity 102 as shown in Figure 2. The additional step of rooting OK2 108 in TA1 100, rather than only using TA1 100 directly is included so that the system operator 226 can revoke the authorisation of any user device 56 at any time without having to change the trust root TA1 100.

The final step undertaken by the system operator 226 is to authorise an application 302 provided by a content provider 52 in step S3. In one example, a content provider 52 submits an application 302 to the system operator 226 for authorisation. The system operator 226 signs the application 302 using the application signing certificate C5 120, which identifies it as an authorised application to all the members of the system 10. Alternatively, the system operator 226 issues the content provider with the C5 certificate 120 and the content provider then signs the application 302 using this certificate. In certain examples, the C5 certificate might be provided by a trusted intermediate certificate authority 106. Steps S1-S3 may occur in any order, or as and when required by the system, for example, when a new content provider 52 is set up.

Steps S4-S7 are preferably performed independently of the system operator 226, with the content provider 52 communicating directly with the user device 56. The authorised / signed application 302 is sent to the user device 56, typically bundled together with the C5 certificate 120, and the certificate C5 120 and signed application 302 are checked in step S4 by the user device 56 so that the user device 56 knows that the application has been authorised. This check involves checking the C5 certificate 120 against TA1 100, which is held by the device 56, and checking the validity of the C5 certificate 120 (such as its expiry date and relevant policies).
The user device 56 then requests content from the content provider 52, using the relevant content provider's application 302. The content provider 52 then checks the authenticity of the user device 56 in step S6 by checking OK2 against TA1, which is also held by the content provider 52. The authenticity of the C5 certificate 120 may also be re-checked at this stage by the device 56 as described above; when running / executing applications 302.

Once the authorisation has been mutually confirmed, content provision can take place. This process may occur in a channel exclusive to the content provider 52 and the user device 56, and may be encrypted. The content provider 52 then sends the content in step S7 via the application 302.

Figure 5 shows the key use and storage in the device 56. In one example, a provisioning authority 54 is authorised by the System Operator 226 and supplies a user device 56 with a set of cryptographic keys. In one example, the provisioning authority 54 is operated or administered by the original equipment manufacturer (OEM) that produces the user device 56.

The user device 56 comprises a System-on-a-Chip (SoC) 60 in combination with local storage 58 and is typically a set-top-box (STB), receiver-decoder, or a personal computer (PC) - or indeed any device adapted to send and receive data, specifically audio/video content. Similarly, content provider 52 may be an audio/video content provider, or any entity which provides data.

25 In this example, the system employs a number of general types of cryptographic keys:

- A single master key (MK) 62
  MK 62 is the highest level cryptographic key, and is the basis (directly or indirectly) for all other public key certificates and keys used by the user device. MK 62 is typically hard-coded during manufacture of device 56 so that other secure keys can be derived from it securely. MK 62 is not accessible to any part of the device 56 apart from the secure processor on the SoC 64. MK 62 is, or is derived from, a device-unique secret which is bound in the SoC 60 during device manufacture.

30 - A set of operational public key certificates (OK) 68
OK 68 are used in the day-to-day running of device 56, for example, during the requesting and receiving of content, and during the execution and updating of software. OK2 108 described above is an example of an operational public key certificate. These certificates can be renewed, changed or revoked by the System Operator 226. These certificates may be provided and renewed in accordance with a user’s subscriptions, or defined by the Content Providers 52 for example. In some embodiments these certificates are provided during manufacture.

A single OK 68 is shown, but in practice there are a number of these, as well as other types of keys, but only a single MK 62.

Further details relating to the authorisation system 10 are now provided.

The described authorisation system and trust model provide the following advantages and/or functionality:

- Protection of Audio/Video (A/V) content using the defined content protection mechanisms, including Digital Rights Management (DRM).
- Allowing content providers to verify that their content is going to a compliant device.
- Protecting the confidentiality of user data.
- Providing a secure means of updating the software on the devices.
- Providing a means to validate configuration data.
- Controlling which applications can run on a client device and granting appropriate access to Application Programming Interfaces (APIs).
- Allowing secure remote management of the devices (where supported and where enabled by the user).

Platform trust hierarchy

The System Operator (226, Figure 1) is responsible for the Platform Trust Hierarchy which is subdivided into several levels which form a hierarchy, each part associated with different aspects or areas of the system. Figure 6 shows an example of a Platform Trust Hierarchy formed by a plurality of operational trusted assets, comprising a Root Certificate Authority 226 and three intermediate Certification Authorities (CA) for: Service and Device Identity 102, Platform Management 104; and Application
Management 106. It should be noted that Figure 6 shows one example of a possible hierarchy and many other examples are within the scope of the invention.

It will be understood that the present invention has been described above purely by way of example, and modifications of detail can be made within the scope of the invention.

Each feature disclosed in the description, and (where appropriate) the claims and drawings may be provided independently or in any appropriate combination.

Reference numerals appearing in the claims are by way of illustration only and shall have no limiting effect on the scope of the claims.
Claims

1. A method of authorising multiple user devices and multiple content providers in a content provision system, the method comprising:
   providing each content provider with a content provider authorisation certificate;
   providing each user device with a user device authorisation certificate, wherein the content provider authorisation certificate and the user device authorisation certificate originate from a common source; and
   determining whether each content provider and each user device is authorised to participate in the content provision system via a mutual exchange and comparison of said certificates between respective content providers and user devices.

2. A method according to Claim 1, wherein the content provider authorisation certificate and the user device authorisation certificate are rooted in a common root certificate.

3. A method according to Claim 2, wherein the common root certificate is a self-signed certificate, preferably following the X.509 standard.

4. A method according to Claim 2 or 3, wherein the root certificate identifies a Root Certificate Authority.

5. A method according to any of Claim 4, further comprising intermediate certificate authorities delegated to act on behalf the Root Certificate Authority.

6. A method according to Claim 5, wherein the intermediate certificate authorities are adapted to provide certificates to the user devices and/or the content providers.

7. A method according to any of Claims 2 to 6, wherein the content provider authorisation certificate and the user device authorisation certificate are signed or generated using a private key of the root certificate.

8. A method according to any of Claims 2 to 7, wherein the content provider and the user device are each further provided with the common root certificate.
9. A method according to Claim 8, wherein the content provider compares the user device authorisation certificate with the common root certificate to determine whether the user device is authorised within the content provision system.

10. A method according to Claim 8 or 9, wherein the user device compares the content provider authorisation certificate with the common root certificate to determine whether the content provider is authorised within the content provision system.

11. A method according to any of the preceding claims, further comprising providing further content providers with content provider authorisation certificates and/or providing further user devices with user device authorisation certificates thereby to add further content providers and/or user devices to the content provision system.

12. A method according to any of the preceding claims, wherein the method employs Public Key Infrastructure (PKI).

13. A method according to any of the preceding claims, further comprising generating a unique content provider authorisation certificate for each content provider and generating a unique user device authorisation certificate for each user device.

14. A method according to Claim 13, wherein the certificates are generated based on the identity of each content provider and each user device.

15. A method according to any of the preceding claims, wherein the certificates are in the form of Public Key Certificates.

16. A method according to any of the preceding claims, wherein the certificates are bound to a public key associated with a particular user device and/or content provider.

17. A method according to any of the preceding claims, further comprising content providers and/or user devices comparing a received certificate with a certificate revocation list.

18. A method according to any of the preceding claims, further comprising
revoking content provider authorisation certificates and/or user device authorisation certificates.

19. A method according to any of the preceding claims, further comprising publishing a list of revoked certificates, which list is accessible by content providers and user devices.

20. A method according to any of the preceding claims, wherein the content provider uses its certificate to sign content provided by said content provider thereby to authenticate or authorise said content to user devices.

21. A method according to any of the preceding claims, further comprising providing, for each content provider, an application adapted to be executed on a user device thereby to enable said user device to interact with said content provider.

22. A method according to Claim 21, further comprising signing said application with the content provider authorisation certificate thereby to authenticate or authorise said application to user devices.

23. A method according to Claim 22, wherein the application is signed by a Root Certificate Authority.

24. A method according to Claim 23, wherein the application is signed by the content provider.

25. A method according to any of Claims 22 to 24, wherein the signed application is provided to the user device via the content provider and/or via a central server forming part of the content provision system.

26. A method according to Claim 25, wherein the signed application is bundled together with the content provider authorisation certificate.

27. A method according to Claim 26, wherein the user device checks the authorisation of the application at any one or more of the following stages: the downloading of the application to the user device; the installation of the application on the user device; and the execution of the application on the user device.
28. A method according to any of Claims 21 to 27, wherein the application enables a content provider to transfer content items, typically audio/visual media items to a user device.

29. A method according to any of Claims 21 to 28, wherein the application enables (direct) communication between the content provider and the user device.

30. A method according to any of Claims 21 to 29, wherein the application enables encrypted communication between the content provider and the user device.

31. A method according to any of the preceding claims, wherein the user device transmits its certificate to a content provider together with a request for content and wherein the content provider checks the authorisation of the user device thereby to determine whether the user device is an authorised user device within the content provision system.

32. A method according to any of the preceding claims, wherein the content provision system is adapted to provide audio/visual media content items to users via a plurality of media content providers, typically broadcast media content providers.

33. A method according to any of the preceding claims, wherein the user device is in the form of a receiver/decoder, for example a Set-Top Box (STB), preferably connectable to a display means such as a television.

34. A method according to any of the preceding claims, further comprising providing the user device with at least one cryptographic key for use in securely acquiring its certificate.

35. A method according to Claim 34, further comprising hard coding the key onto the user device.

36. A system for authorising multiple user devices and multiple content providers in a content provision system, the system comprising:

35 means for providing each content provider with a content provider authorisation certificate;
means for providing each user device with a user device authorisation certificate, wherein the content provider authorisation certificate and the user device authorisation certificate originate from a common source; and
means for determining whether each content provider and each user device is authorised to participate in the content provision system via a mutual exchange and comparison of said certificates between respective content providers and user devices.

37. A system according to Claim 36, wherein the or each user device is in the form of a receiver/decoder, for example a Set Top Box (STB), preferably connectable to a display means such as a television.

38. A system according to Claim 37, wherein the or each user device and/or content provider is connectable to a communication network.

39. A system according to any of Claims 36 to 38, further comprising a central server comprising means for generating or signing the certificates.

40. A system according to Claim 39, wherein the server is connectable to a communication network.

41. A system according to Claim 39 or 40, wherein the server is adapted to function as a Root Certificate Authority in a PKI system.

42. A receiver/decoder adapted to form part of the system according to any of Claims 36 to 41 or to carry out any of the method steps according to Claims 1 to 35.

43. A computer program product comprising software code adapted, when executed on a data processing apparatus, to perform any of the steps of the method according to any of Claims 1 to 35.

44. A method substantially as herein described and/or as illustrated with reference to the accompanying diagrammatic drawings.

45. A system substantially as herein described and/or as illustrated with reference to the accompanying diagrammatic drawings.
46. A receiver/decoder substantially as herein described and/or as illustrated with reference to the accompanying diagrammatic drawings.

47. A computer program product substantially as herein described and/or as illustrated with reference to the accompanying diagrammatic drawings.
Figure 2
Figure 4

Possible intermediate entity

Encrypted communication
Figure 6