Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2393685 A1 2004/01/16

(21) 2 393 685

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2002/07/16

(41) Mise à la disp. pub./Open to Public Insp.: 2004/01/16

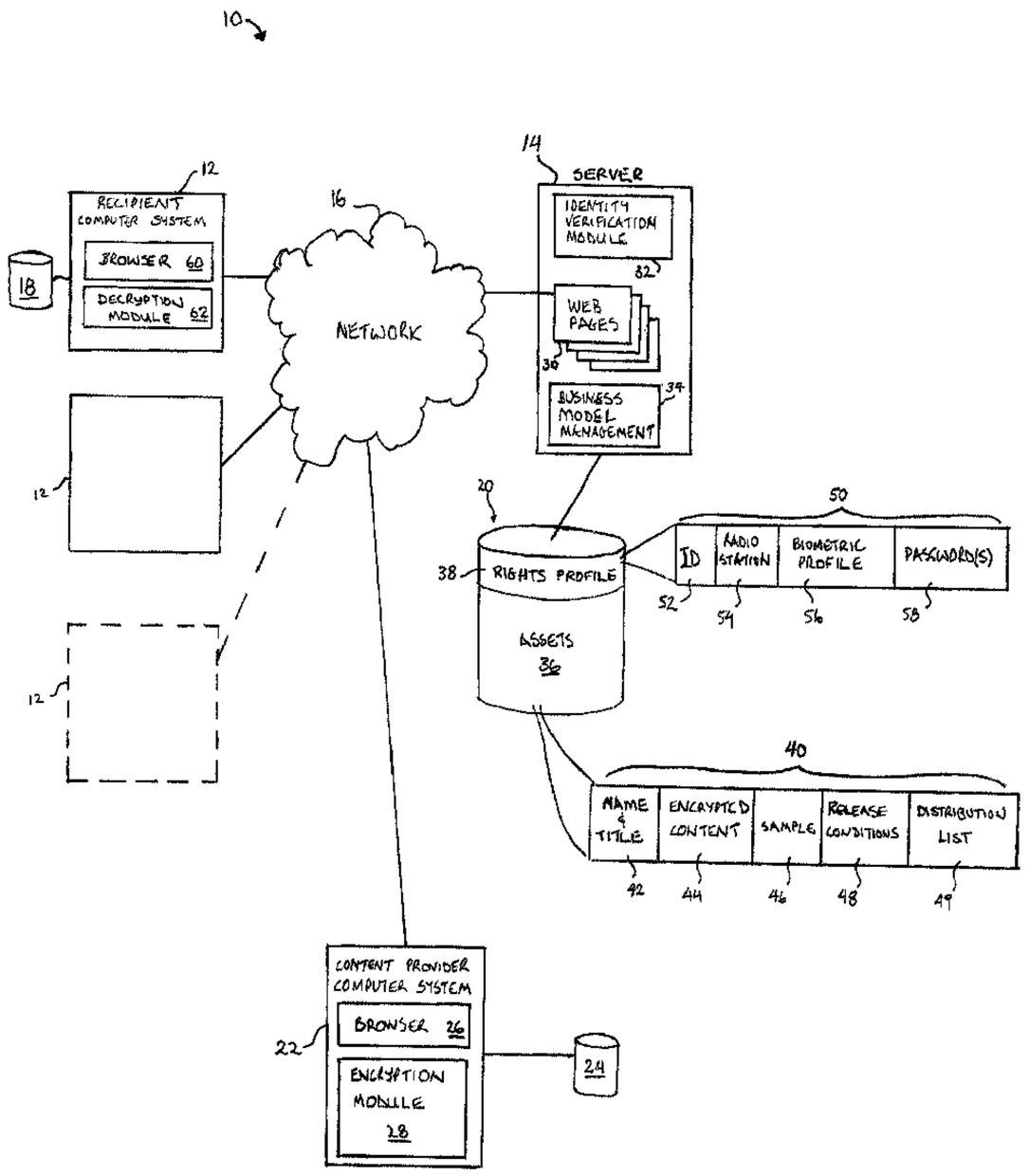
(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 9/32, G06F 17/30

(71) Demandeur/Applicant:
MUSICRYPT INC., CA

(72) Inventeurs/Inventors:
HEAVEN, JOHN, CA;
HOCH, WOJTEK, CA;
HUNT, CLIFF, CA

(74) Agent: RIDOUT & MAYBEE LLP

(54) Titre : SYSTEME ET METHODE DE DISTRIBUTION DE CONTENU
(54) Title: CONTENT DISTRIBUTION SYSTEM AND METHOD



(57) Abrégé/Abstract:
A method and system for the secure distribution of content to authorized persons. A content provider uploads encrypted content to the system and specifies the institutions or individuals to which the content is to be provided and release conditions under which it is to be made available. Encrypted content is made available to a recipient together with a decryption code, if the identity of the recipient can be confirmed through a validation procedure and if the release conditions are met. The release conditions may include a time and date at which the release is to occur. The encrypted content have an associated sample which may be streamed to the recipient so as to permit the recipient to assess whether to download the full encrypted content or not. In one embodiment, the validation procedure includes biometric validation of the identity of the recipient.

ABSTRACT

A method and system for the secure distribution of content to authorized persons. A content provider uploads encrypted content to the system and specifies the institutions or individuals to which the content is to be provided and release conditions under which it is to be made available. Encrypted content is made available to a recipient together with a decryption code, if the identity of the recipient can be confirmed through a validation procedure and if the release conditions are met. The release conditions may include a time and date at which the release is to occur. The encrypted content have an associated sample which may be streamed to the recipient so as to permit the recipient to assess whether to download the full encrypted content or not. In one embodiment, the validation procedure includes biometric validation of the identity of the recipient.

CONTENT DISTRIBUTION SYSTEM AND METHOD

FIELD OF THE INVENTION

[0001] This invention relates to the distribution of content to remote locations over a network, and more particularly to the secure distribution of content to authorized persons.

BACKGROUND OF THE INVENTION

[0002] The security and timing of the release of promotional material can be of vital importance to the developers of that material. For example, in the music industry a key component of marketing is the release of a single off a new album to radio stations. The listener response to a new single provides important information upon which wider marketing and release decisions will be based. For radio stations, the release of a new single also provides them with a promotional event to boost market share. Being the first station to premiere a new single by a popular artist can provide a competitive advantage.

[0003] Accordingly, controlling the timing of the release of a single and the persons receiving it is an important aspect of a recording label promotional program. Traditionally, the distribution is done by creating a promotion-only CD containing the single track and then distributing this CD to individual radio stations by courier. This method has many drawbacks, including the number of people who handle the CD while it is in transit. In many instances, a new single has been illicitly copied or stolen, distributed to unauthorized persons and released to the public prior to the intended release date and time. Moreover, this method is

difficult to time accurately, is labour-intensive and subject to disruption from weather, labour strife, transportation problems and human error. Ensuring that competitive radio stations have access to a new single simultaneously and securely is important to the trust between the record label and the radio stations.

[0004] The same difficulties can be found in other industries and circumstances, including the distribution of new movies in the film industry, the distribution of new campaigns in the advertising industry, or the distribution of new financing promotions in the auto sales industry. In general, the problem is experienced in any industry in which a content provider wishes to ensure the security and simultaneous timing of a distribution of content to a plurality of recipients.

SUMMARY OF THE INVENTION

[0005] The present invention provides a method and system for the secure distribution of content to authorized persons. A content provider uploads encrypted content to the system and specifies the institutions or individuals to which the content is to be provided and release conditions under which it is to be made available. Encrypted content is made available to a recipient together with a decryption code, if the identity of the recipient can be confirmed through a validation procedure and if the release conditions are met. The release conditions may include a time and date at which the release is to occur. In one embodiment, the validation procedure includes biometric validation of the identity of the recipient.

[0006] In one aspect, the present invention provides a method of

distributing content to a plurality of recipients from a database over a distributed computer network, each recipient having a terminal connected to the network, and the database containing an encrypted content file. The method includes verifying the identity of a recipient and permitting the selection of an encrypted content file by the recipient. If the recipient's identify is verified, then the method includes downloading the selected encrypted content file to the recipient and decrypting the encrypted content file. In one embodiment, the recipient may review one or more samples of the content prior to downloading and decrypting the content file, and may tag the files in which the recipient is interested.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Reference will now be made, by way of example, to the accompanying drawings which show an embodiment of the present invention, and in which:

[0008] Figure 1 shows a block diagram of an embodiment of a content distribution system according to the present invention;

[0009] Figure 2 shows a flowchart outlining an embodiment of the steps for loading content into a distribution system according to the present invention; and

[0010] Figure 3 shows a flowchart outlining an embodiment of the steps for distributing content to recipients according to the present invention.

DESCRIPTION OF SPECIFIC EMBODIMENTS

[0011] Reference is first made to Figure 1, which shows a block diagram of an embodiment of a content distribution system 10 according to the present invention. A plurality of recipient computer systems 12 and a remote distribution server 14 are mutually connected via a communications network 16, such as the Internet. Also connected to the communications network 16 is a content provider computer system 22. The content provider computer system 22 provides content to the server 14 for distribution to the recipient computer systems 12, as is further detailed below. In one embodiment, as described herein, the content is pre-recorded digital music provided by a record label promotions director for distribution to radio stations, however it will be understood that the present invention is not limited to this embodiment. The content is not limited to music and may include other content, such as text, audio, video, computer software, or visual media like advertising and promotions. Other content will be understood by those skilled in the art upon a review of the following description of the present invention.

[0012] The content provider computer system 22 may be any conventional personal computer. The content provider computer system 22 is connected to a storage medium 24 containing the content intended for distribution to the recipient computer systems 12. The storage medium 24 may include ROM, RAM, floppy discs, compact discs, digital tape or any other medium on which content may be stored. The content provider computer system 22 includes a browser 26 for accessing web pages through the communications network 16. The content provider computer system 22 also includes an encryption module 28 for encoding, encrypting and uploading the content. It will be understood that the content provider computer system 22 may have more or fewer components than, or

alternative components to, those shown in Figure 1 and still provide the same functionality described herein.

[0013] Similarly, the recipient computer system 12 may be any conventional personal computer. The recipient computer system 12 also includes a browser 60 for accessing web pages through the communication network 16. The recipient computer system 12 includes a decryption module 62 for decrypting content obtained from the remote distribution server 14. The recipient computer system 12 is connected to a storage device 18 for storing any encrypted or decrypted content. In one embodiment, the storage device 18 is a mass storage device containing music in WAV format for use in radio broadcasts. Again, it will be understood that the recipient computer system 12 may have more or fewer components and still provide the same functionality described herein.

[0014] The remote distribution server 14 is configured to receive encrypted content from the content provider computer system 22 and to distribute the content to individual recipient computer systems 12, subject to verification of the identity of the user of the recipient computer system 12 and to the release time or date restrictions imposed by the user of the content provider computer system 22. The remote distribution server 14 ensures that decrypted content is not provided to unauthorized individuals or provided before the release time and date.

[0015] The remote distribution server 14 includes web pages 30 to provide a graphical user interface with the content provider computer system 22 and the recipient computer systems 12. The remote distribution server 14 also includes an identity verification module 32 and a business model management module 34. Connected to and accessible to the remote distribution server 14 is a mass storage device 20. The mass storage device 20 includes a rights profile database 38 and

an asset database 36.

[0016] The identity verification module 32 permits access to the content distribution system 10 to be controlled based upon biometric verification of the identity of an individual using either a recipient computer system 12 or a content provider computer system 22. Verification of the individual's identity is accomplished by comparing the characteristics of the individual's typing cadence with a previously stored profile of the same activity collected during a registration process which involves reiterative entry of the same password or passphrase. An example of a keystroke dynamics biometric identity verification system can be seen in US Patent No. 4,805,222, which has been assigned to Net Nanny Inc. of Vancouver, B.C., Canada. In one embodiment of the present invention, the identify verification module 32 compares the individual's e-mail address, user name and password as well as biometric data, to prevent unauthorized access. By limiting distribution of content to particular individuals through validating the identity of the individuals, rather than the identity of a particular computer system, the possibility of unauthorized access to the content is minimized. In the context of a radio station, only one or two individuals at a particular radio station may be authorized to access content on the system 10.

[0017] The rights profile database 38 includes a database of individual user profiles for those users that have registered to access the system 10, either as recipients or content providers. Each entry 50 in the rights profile database 38 may include identification information 52, such as user name, e-mail address or other identifying information. Each entry 50 may also include, in this embodiment, a radio station 52 with which the individual user is associated. Also included in each user entry 50 is biometric data 56 for use by the identity verification module 32 and one or more passwords 58. Further or other

information may be included in the entries 50.

[0018] The asset database 36 includes the securely encrypted content provided by various content providers. Each entry 40 in the database includes song identification information 42 such as the artist's name, the title of the song and other information. Also included is a pointer or address information 44 for accessing the encrypted digital music single in the database. The entry 40 may also include a streaming unencrypted sample 46 of the music single. The sample allows a recipient to evaluate and pre-screen new upcoming singles and make programming decisions. The entry 40 also includes a release time and date 48 and a distribution list 49 of recipients that will be granted access to the digital music single. In one embodiment, the entry 40 includes an associated graphic (not shown), such as a photo, artist logo or album cover. The entry 40 may also include a pointer to an associated video (not shown) that may be downloaded with the digital music single or streamed to the recipient computer system 12. Further or other information may be included in the entries 40.

[0019] The business model management module 34 controls access to content of the asset database 36 based upon the distribution list 49 and the user profiles in the rights profile database 38, and it performs billing and reporting functions.

[0020] In operation, a content provider, such as a record label promotions director, uses the content provider computer system 22 to upload an encrypted digital music single to the remote distribution server 14. Reference is made to Figure 2, which shows a flowchart 100 outlining an embodiment of the steps for loading content upon the server 14. To begin the process, the content provider uses the encryption module 28 to select content from the storage medium 24 (step

100-1). The storage medium 24 may be the artist's unreleased CD placed in the CD drive of the content provider computer system 22. The encryption module 28 is then employed to compress (step 100-2) and encrypt (100-3) the content. The content having been selected, compressed and encrypted, the encryption module 28 causes the browser 26 to be launched and to access the web pages 30 provided by the server 14 (step 100-4). The web pages 30 to which the encryption module 28 directs the browser 26 step the content provider through the process of uploading the encrypted digital file.

[0021] To upload a track, the content provider enters identification data 42 (step 100-5), such as the name of the track and the artist's name. Other information may be entered, such as the length of the track or the title of an associated album. The content provider then chooses a release time and date 48 (step 100-6). The content provider next selects a distribution list 49 of the individuals or radio stations that will be entitled to receive the single (step 100-7). The encrypted content is then uploaded to the server 14 for storage on the mass storage device 20 (step 100-8). If there are associated graphics or video for distribution with the encrypted digital music single, then those are also uploaded to the server 14. The server 14 assesses whether the transfer was successful (step 100-9) and sends an error message (step 100-10) to the content provider computer system 22 if the upload failed. If successful, the server 14 sends a confirmation to the content provider computer system 22 (step 100-11). The server 14 may also send a notification to the recipients in the distribution list 49 to alert them to existence of an upcoming single release.

[0022] Figure 3 shows a flowchart 200 outlining an embodiment of the steps for distributing content to recipients. A radio station music director, for example, may access a new single release through the content distribution system

10 by using a recipient computer system 12. The music director may employ the browser 60 to access the web pages 30 on the server 14 (step 200-1). If the music director has a user profile in the rights profile database 38 then he or she may log on using their biometric password (step 200-2). The identity verification module 32 will verify their identity. If the music director does not have a valid user profile, then he or she will be directed through a registration process to establish a user profile (step 200-3).

[0023] Once the identity of the music director has been verified, the system 10 accesses the assets database 36 and the rights profile database 38 and determines which singles have a distribution list 49 that includes the music director or his radio station (step 200-4). The system 10 will then display information regarding the singles that the music director is entitled to access (step 200-5).

[0024] In one embodiment, the information will include singles prior to their release date. The music director may choose to listen to sample tracks (step 200-6), which are then streamed unencrypted to the recipient computer system, for example in MP3 format (step 200-7). These sample tracks are of insufficient length or quality to be used for radio play and, thus, pose little risk insofar as the security of the single is concerned. The system 10 may permit the music director to tag or select singles as "favorites" or "notables", allowing a music director to sort through hundreds of samples and easily return to those which require further consideration or download. Such a feature may also permit the music director to save his or her preferences so as to preserve the list of tagged files.

[0025] The music director may choose to download (step 200-8) any full length singles to which he or she has authorized access provided the single release

time/date has been reached. If the release conditions are not met (step 200-9), the music director will receive an error notification informing him or her of the date and time at which they may return to download the single. In another embodiment, the music director may be permitted to download encrypted singles prior to the release date, but will not be provided with the decryption code for decrypting the singles until the release date and time. Singles are downloaded (step 200-10) in encrypted compressed WAV format and are decrypted and de-compressed on the recipient computer system 12 using the decryption module 62 and the decryption code provided by the server 14.

[0026] The present invention may be embodied in other specific forms without departing from the spirit or essential characteristics thereof. Certain adaptations and modifications of the invention will be obvious to those skilled in the art. Therefore, the above discussed embodiments are considered to be illustrative and not restrictive, the scope of the invention being indicated by the appended claims rather than the foregoing description, and all changes which come within the meaning and range of equivalency of the claims are therefore intended to be embraced therein.

WHAT IS CLAIMED IS:

1. A method of distributing content to a plurality of recipients from a database over a distributed computer network, each recipient having a terminal connected to the network, the database containing an encrypted content file, comprising the steps of:

(a) verifying the identity of one of said recipients;

(b) permitting the selection of said encrypted content file by said one of said recipients;

(c) downloading said selected encrypted content file to the terminal of said one of said recipients; and

(d) if said recipient's identity is verified, decrypting said selected encrypted content file.

2. The method claimed in claim 1, wherein said step of verifying includes obtaining a biometric input from said recipient and comparing said biometric input with a stored biometric profile.

3. The method claimed in claim 2, wherein said biometric input includes said recipient's typing cadence.

4. The method claimed in claim 1, wherein said encrypted content file includes digital music.

5. The method claimed in claim 4, wherein said plurality of recipients includes a plurality of radio stations.

6. The method claimed in claim 1, wherein said database further contains a release condition, and wherein said method further includes a step of verifying that said release condition is met prior to said step of decrypting.

7. The method claimed in claim 6, wherein said release condition includes a time and a date before which said step of decryption cannot be performed.

8. The method claimed in claim 1, further including the steps of receiving said list of the plurality of recipients and said encrypted content file for storage on the database, and notifying the plurality of recipients of said receipt.

9. The method claimed in claim 1, wherein the database further includes an unencrypted sample associated with said encrypted content file and wherein said method further includes a step of streaming said unencrypted sample to the terminal of said one of said recipients.

10. The method claimed in claim 1, wherein the database further includes a graphical file associated with said encrypted content file and wherein the method further includes a step of streaming or downloading said graphical file to the terminal of said one of said recipients.

11. The method claimed in claim 1, wherein the database further includes a video file associated with said encrypted content file and wherein the method further includes a step of streaming or downloading said video file to the terminal of said one of said recipients.

12. A method of distributing content to a plurality of recipients from a database over a distributed computer network, each recipient having a terminal connected to the network, the database containing an encrypted content file, comprising the steps of:

(a) verifying the identity of said one of said recipients;

(b) permitting the selection of said encrypted content file by one of said recipients;

(c) if said recipient's identity is verified, downloading said selected encrypted content file to the terminal of said one of said recipients and decrypting said selected encrypted content file.

13. The method claimed in claim 12, wherein said step of verifying includes obtaining a biometric input from said recipient and comparing said biometric input with a stored biometric profile.

14. The method claimed in claim 13, wherein said biometric input includes said recipient's typing cadence.

15. The method claimed in claim 12, wherein said encrypted content file includes digital music.

16. The method claimed in claim 15, wherein said plurality of recipients includes a plurality of radio stations.

17. The method claimed in claim 12, wherein said database further contains a release condition, and wherein said method further includes a step of verifying that said release condition is met prior to said step of downloading and decrypting.

18. The method claimed in claim 17, wherein said release condition includes a time and a date before which said step of downloading and decryption cannot be performed.

19. The method claimed in claim 12, further including the steps of receiving said list of the plurality of recipients and said encrypted content file for storage on the database, and notifying the plurality of recipients of said receipt.

20. The method claimed in claim 12, wherein the database further includes an unencrypted sample associated with said encrypted content file and wherein said method further includes a step of streaming said unencrypted sample to the terminal of said one of said recipients.

21. The method claimed in claim 12, wherein the database further includes a graphical file associated with said encrypted content file and wherein the method further includes a step of streaming or downloading said graphical file to the terminal of said one of said recipients.

22. The method claimed in claim 12, wherein the database further includes a video file associated with said encrypted content file and wherein the method further includes a step of streaming or downloading said video file to the terminal of said one of said recipients.

23. A system for distributing content to a plurality of recipients over a distributed computer network, the system comprising:

(a) a server connected to said network and including a database having an encrypted content file, a selection module for permitting one of said recipients to select said encrypted digital media file, and a verification module for verifying the identity of said one of said recipients; and

(b) a terminal connected to said network and having an input means for

providing input to said verification module and a storage means for receiving said selected encrypted content file,

wherein said server includes a download module for sending said selected encrypted content file to said terminal in response to an identity verification by said verification module; and

(c) a decryption module for decrypting said selected content file at said terminal.

24. The system claimed in claim 23, wherein said verification module includes a biometric verification module for verifying an individual's identity using biometric input.

25. The system claimed in claim 24, wherein said input means includes a keyboard and said biometric verification module includes a typing cadence identity verification module.

26. The system claimed in claim 23, wherein said database further has an unencrypted sample associated with said encrypted content file, and wherein said server includes a sample streaming module for streaming said unencrypted sample to said terminal.

Ridout & Maybee LLP
Suite 2400
One Queen Street East
Toronto, Canada M5C 3B1
Patent Agents of the Applicant

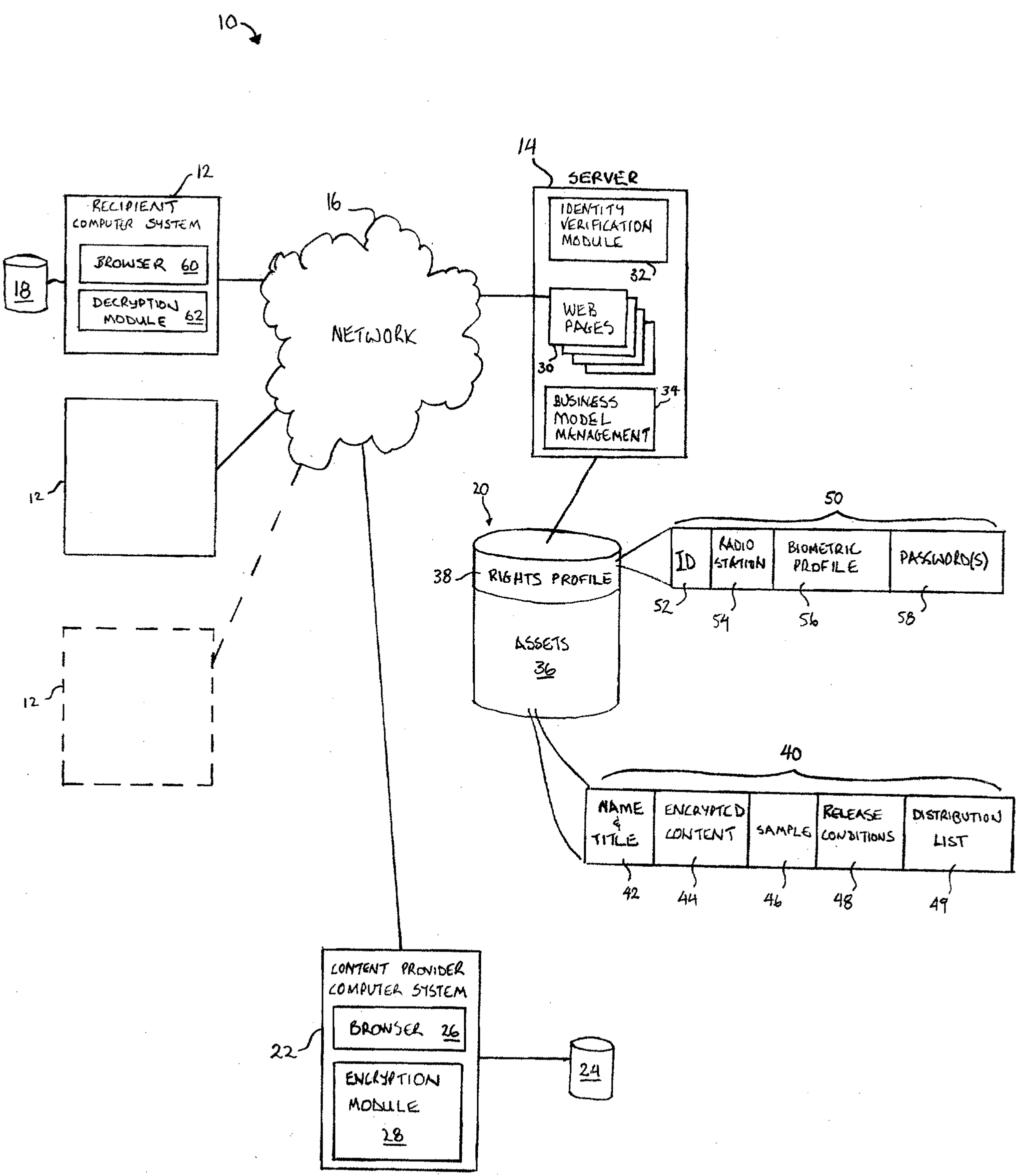

10
14
12
RECIPIENT COMPUTER SYSTEM
BROWSER 60
DECRYPTION MODULE 62
18
16
NETWORK
SERVER
IDENTITY VERIFICATION MODULE
32
WEB PAGES
30
BUSINESS MODEL MANAGEMENT
34
12
12
20
38
RIGHTS PROFILE
ASSETS
36
50
ID
RADIO STATION
BIOMETRIC PROFILE
PASSWORD(S)
52
54
56
58
40
NAME & TITLE
ENCRYPTED CONTENT
SAMPLE
RELEASE CONDITIONS
DISTRIBUTION LIST
42
44
46
48
49
CONTENT PROVIDER COMPUTER SYSTEM
BROWSER 26
ENCRYPTION MODULE 28
22
24

FIGURE 1

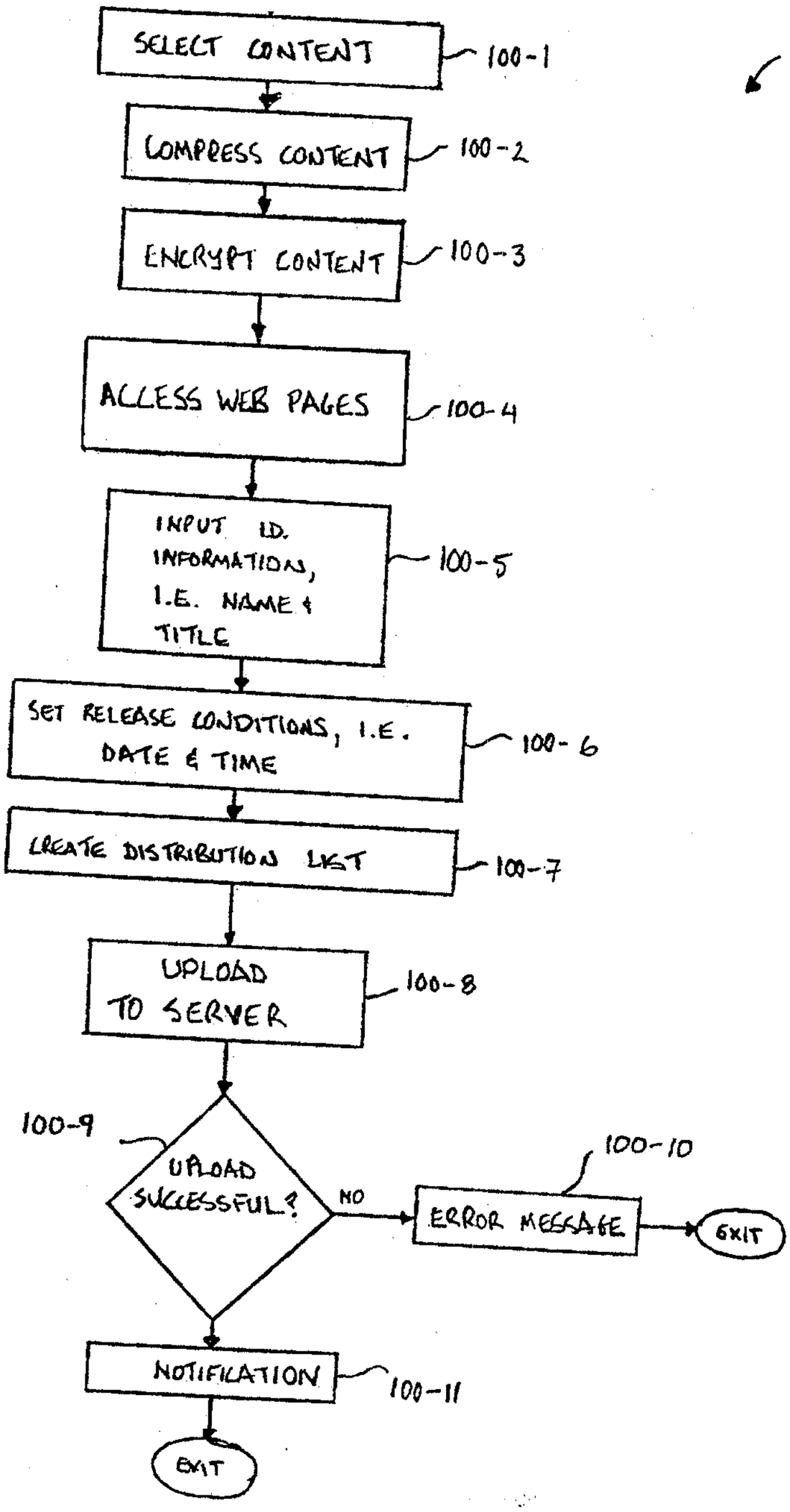

SELECT CONTENT
100-1
100
COMPRESS CONTENT
100-2
ENCRYPT CONTENT
100-3
ACCESS WEB PAGES
100-4
INPUT I.D. INFORMATION, I.E. NAME & TITLE
100-5
SET RELEASE CONDITIONS, I.E. DATE & TIME
100-6
CREATE DISTRIBUTION LIST
100-7
UPLOAD TO SERVER
100-8
100-9
UPLOAD SUCCESSFUL?
NO
100-10
ERROR MESSAGE
EXIT
NOTIFICATION
100-11
EXIT

FIGURE 2

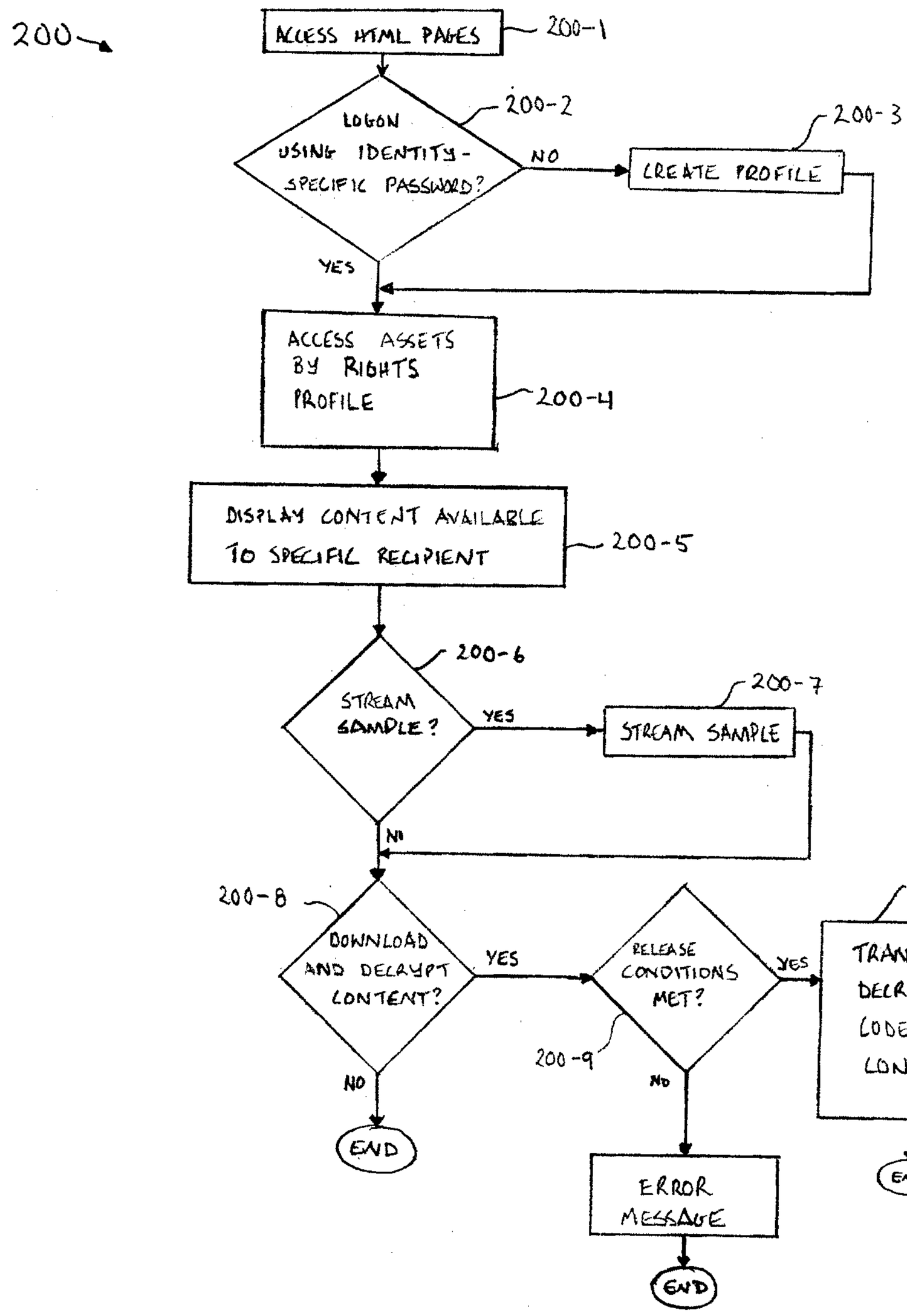
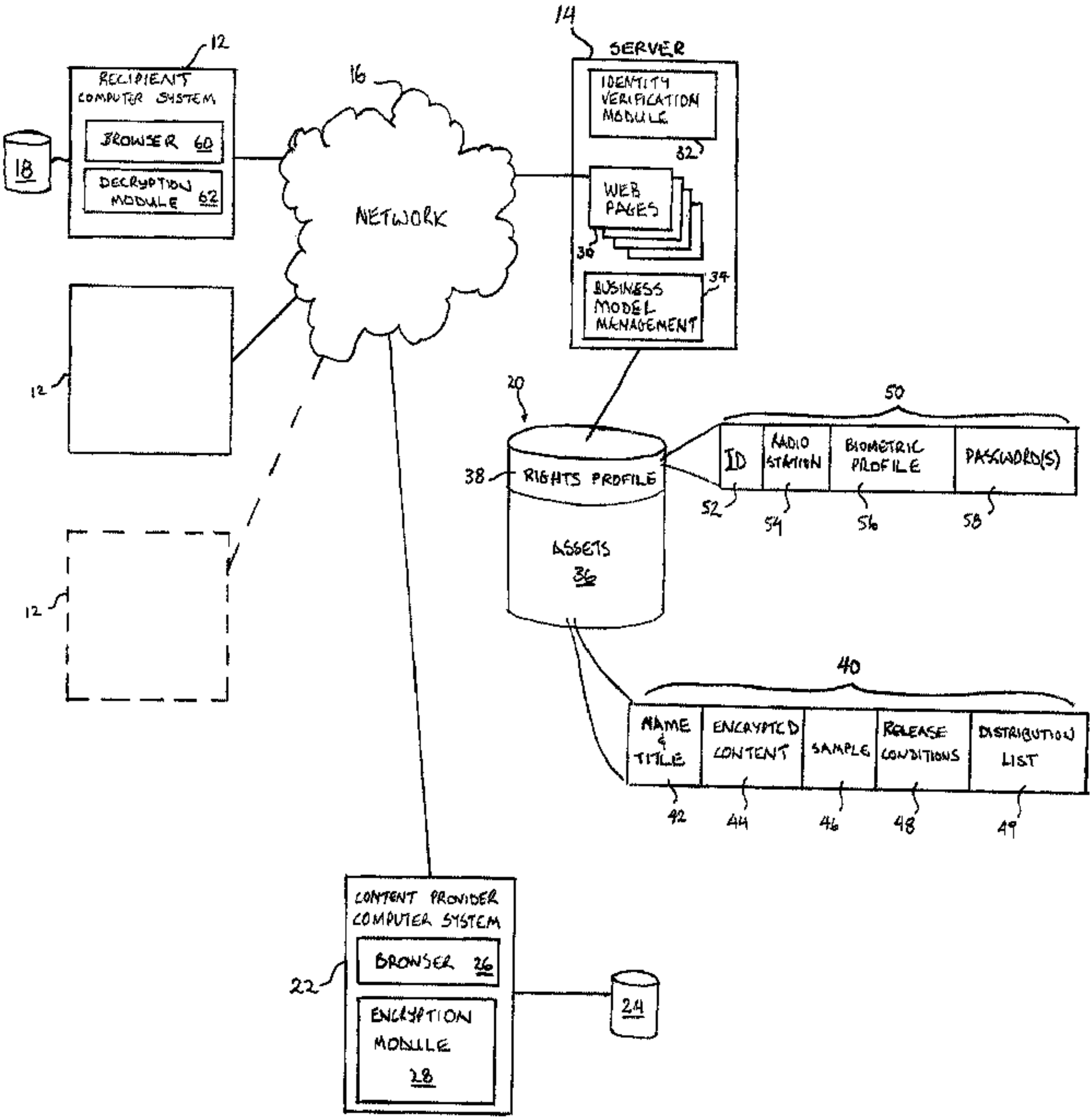

200
ACCESS HTML PAGES
200-1
LOGON USING IDENTITY-SPECIFIC PASSWORD?
200-2
NO
200-3
CREATE PROFILE
YES
ACCESS ASSETS BY RIGHTS PROFILE
200-4
DISPLAY CONTENT AVAILABLE TO SPECIFIC RECIPIENT
200-5
200-6
STREAM SAMPLE?
YES
200-7
STREAM SAMPLE
NO
200-8
DOWNLOAD AND DECRYPT CONTENT?
YES
RELEASE CONDITIONS MET?
200-9
YES
200-10
TRANSFER DECRYPTION CODE AND CONTENT
NO
END
NO
ERROR MESSAGE
END
END

FIGURE 3


10
12
RECIPIENT COMPUTER SYSTEM
BROWSER 60
DECRYPTION MODULE 62
18
16
NETWORK
14
SERVER
IDENTITY VERIFICATION MODULE
82
WEB PAGES
30
BUSINESS MODEL MANAGEMENT
34
12
12
20
38
RIGHTS PROFILE
ASSETS
36
50
ID
RADIO STATION
BIOMETRIC PROFILE
PASSWORD(S)
52
54
56
58
40
NAME & TITLE
ENCRYPTED CONTENT
SAMPLE
RELEASE CONDITIONS
DISTRIBUTION LIST
42
44
46
48
49
CONTENT PROVIDER COMPUTER SYSTEM
22
BROWSER 26
ENCRYPTION MODULE 28
24