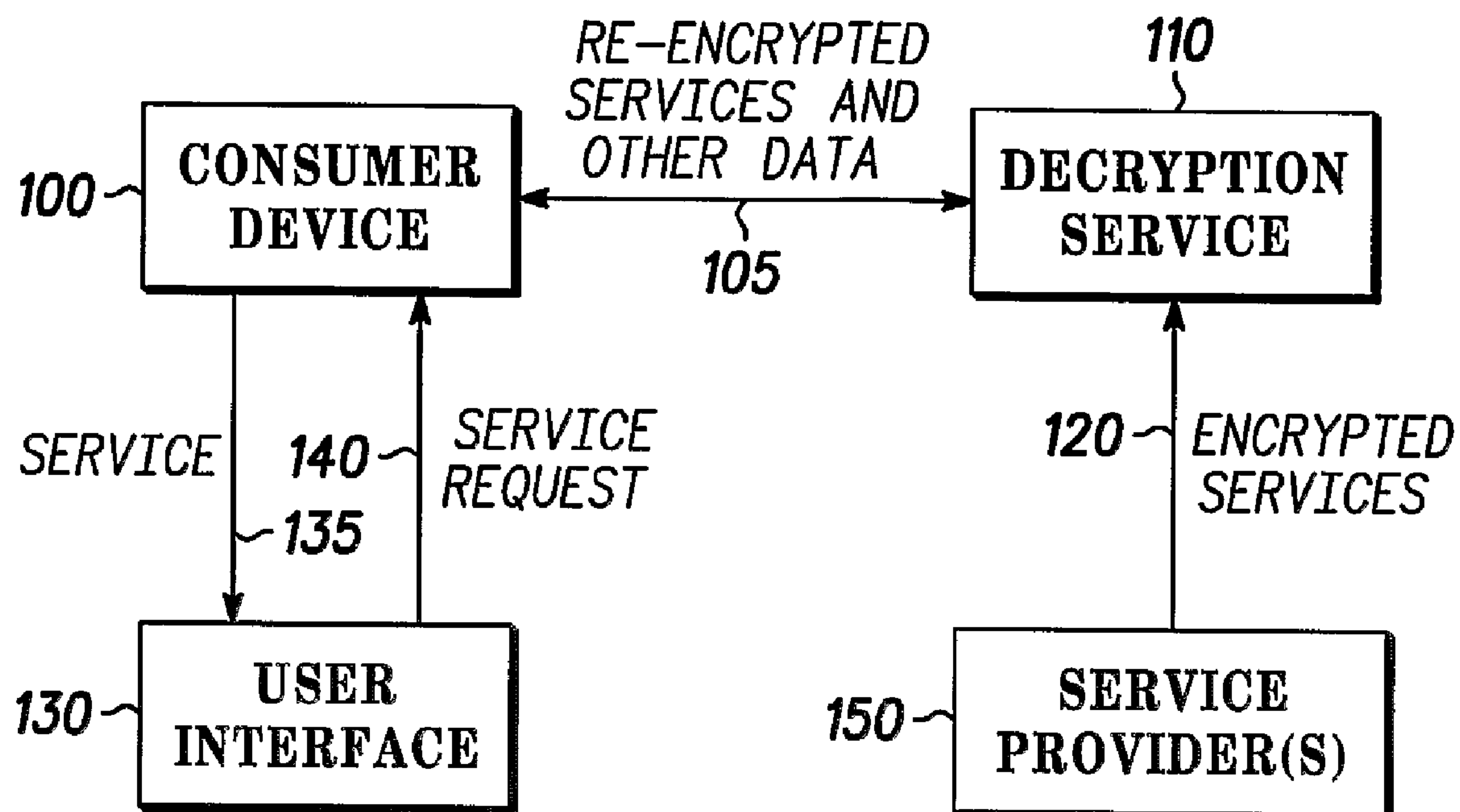




(86) Date de dépôt PCT/PCT Filing Date: 2004/02/12
(87) Date publication PCT/PCT Publication Date: 2004/09/02
(45) Date de délivrance/Issue Date: 2013/06/18
(85) Entrée phase nationale/National Entry: 2005/07/28
(86) N° demande PCT/PCT Application No.: US 2004/004308
(87) N° publication PCT/PCT Publication No.: 2004/075530
(30) Priorité/Priority: 2003/02/19 (US10/368,845)

(51) Cl.Int./Int.Cl. *H04L 29/06* (2006.01)
(72) Inventeur/Inventor:
BOOTH, ROBERT C., US
(73) Propriétaire/Owner:
GENERAL INSTRUMENT CORPORATION, US
(74) Agent: GOWLING LAFLEUR HENDERSON LLP

(54) Titre : PROCEDES ET APPAREIL POUR L'INTEGRATION DE SYSTEMES DE SECURITE UNIDIRECTIONNEL ET BIDIRECTIONNEL POUR ASSURER LA DISTRIBUTION SECURISEE DE SERVICES CHIFFRES
(54) Title: METHODS AND APPARATUS FOR INTEGRATING ONE-WAY AND TWO-WAY SECURITY SYSTEMS TO ENABLE SECURE DISTRIBUTION OF ENCRYPTED SERVICES



(57) **Abrégé/Abstract:**

The present invention provides methods and apparatus for integrating one-way and two-way security systems to enable secure distribution of services. A decryption device (110) securely receives and decrypts encrypted services from one or more service providers (150). A consumer device (100) securely communicates with the decryption device (110). A user interface (130) associated with the consumer device (100) initiates a service request (140) for a requested service from a service provider (150). In operation, the service request (140) is communicated from the consumer device (100) to the decryption device (110). The requested service (140) is then acquired by the decryption device (110) as an encrypted requested service (120). The acquired requested service (120) is then decrypted by the decryption device (110). The requested service (120) is re-encrypted and securely communicated from the decryption device (110) to the consumer device (100). The re-encrypted requested service (105) is then decrypted and decoded at the consumer device (100) to provide the requested service.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
2 September 2004 (02.09.2004)

PCT

(10) International Publication Number
WO 2004/075530 A3

(51) International Patent Classification⁷: **H04L 29/06**

(21) International Application Number:
PCT/US2004/004308

(22) International Filing Date: 12 February 2004 (12.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/368,845 19 February 2003 (19.02.2003) US

(71) Applicant (for all designated States except US): **GENERAL INSTRUMENT CORPORATION** [US/US]; 101 Tournament Drive, Horsham, PA 19044 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **BOOTH, Robert, C.** [US/US]; 1700 Rockcress Drive, Jamison, PA 18929 (US).

(74) Agents: **SILVERIO, John V.** et al.; Motorola, Inc., 101 Tournament Drive, Horsham, PA 19044 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,

CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

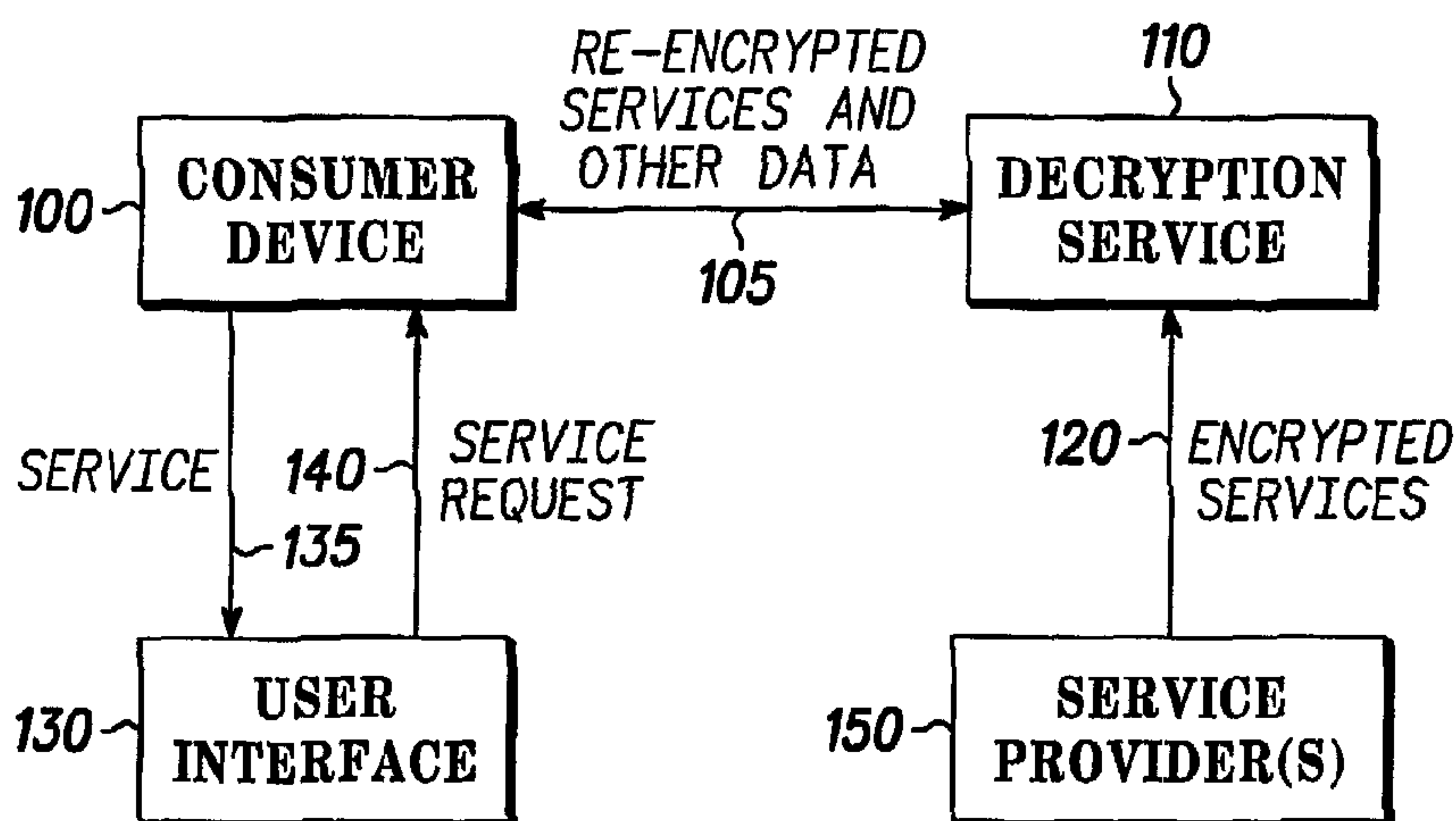
- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

(88) Date of publication of the international search report:

28 October 2004

[Continued on next page]

(54) Title: METHODS AND APPARATUS FOR INTEGRATING ONE-WAY AND TWO-WAY SECURITY SYSTEMS TO ENABLE SECURE DISTRIBUTION OF ENCRYPTED SERVICES



(57) Abstract: The present invention provides methods and apparatus for integrating one-way and two-way security systems to enable secure distribution of services. A decryption device (110) securely receives and decrypts encrypted services from one or more service providers (150). A consumer device (100) securely communicates with the decryption device (110). A user interface (130) associated with the consumer device (100) initiates a service request (140) for a requested service from a service provider (150). In operation, the service request (140) is communicated from the consumer device (100) to the decryption device (110). The requested service (140) is then acquired by the decryption device (110) as an encrypted requested service (120). The acquired requested service (120) is then decrypted by the decryption device (110). The requested service (120) is re-encrypted and securely communicated from the decryption device (110) to the consumer device (100). The re-encrypted requested service (105) is then decrypted and decoded at the consumer device (100) to provide the requested service.

WO 2004/075530 A3

WO 2004/075530 A3



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

**METHODS AND APPARATUS FOR INTEGRATING ONE-WAY AND
TWO-WAY SECURITY SYSTEMS TO ENABLE SECURE DISTRIBUTION OF
ENCRYPTED SERVICES**

BACKGROUND OF THE INVENTION

5 The present invention relates to the fields of digital and streaming media communications, in-home networking, and digital communication security. More specifically, the present invention relates to the integration of one-way and two-way security systems to enable the secure distribution of encrypted services.

 Television system operators, including cable and satellite television system
10 operators, as well as off-air service providers, offer a large number of audio, video, and audiovisual services to their customers. Such services include standard television programming, pay-per-view television programming, on-demand programming, streaming media services, Internet services, and the like. However, the consumers receiving such services are typically limited to viewing the services on a particular television set
15 associated with a television terminal (e.g., set-top box) provided by the television system operator.

 Currently there is no mechanism to securely distribute encrypted audio and/or video content from a digital television terminal (such as a digital set-top box) to a remote television set or other consumer device in a manner that protects the interests of the content
20 provider and the television system operator.

 It would be advantageous to establish a secure environment for distributing audio and/or video content beyond the television terminal. It would be further advantageous if such distribution could be accomplished using an in-home network, by integrating a one-way security system provided, for example, in the television terminal, with a two-way
25 security system provide, for example, in a web pad. Enabling such distribution would make television system operators more receptive to purchasing new products, such as web pads and the like. Further, television system operators would be able to assess additional service charges for such capability, as consumers would be able use their personal computers (or a web pad, or the like) to access services from their television terminals via the in-home
30 network. Such a feature would drive the sales of television terminals that are so enabled.

The methods and apparatus of the present invention provide the foregoing and other advantages.

SUMMARY OF THE INVENTION

The present invention relates to methods and apparatus for integrating one-way and two-way security systems to enable secure distribution of services. A decryption device is provided which is enabled to securely receive and decrypt encrypted services from one or more service providers. A consumer device is provided which is enabled to securely communicate with the decryption device. A user interface associated with the consumer device is provided for initiating a service request for a requested service from the one or more service providers. In operation, the service request is communicated from the consumer device to the decryption device. The requested service is then acquired by the decryption device from the one or more service providers in response to the service request as an encrypted requested service. The acquired encrypted requested service is then decrypted by the decryption device. The requested service is re-encrypted and securely communicated from the decryption device to the consumer device. The re-encrypted requested service can then be decrypted and decoded at the consumer device to provide the requested service.

Those skilled in the art will appreciate that the present invention may be implemented using software, hardware, and/or firmware.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will hereinafter be described in conjunction with the appended drawing figures, wherein like numerals denote like elements, and:

Figure 1 shows a block diagram of an example embodiment of the present
5 invention;

Figure 2 shows a block diagram of an example embodiment of a decryption device in accordance with the present invention; and

Figure 3 shows a block diagram of an example embodiment of a consumer device in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The ensuing detailed description provides preferred exemplary embodiments only, and is not intended to limit the scope, applicability, or configuration of the invention. Rather, the ensuing detailed description of the preferred exemplary embodiments will
 5 provide those skilled in the art with an enabling description for implementing a preferred embodiment of the invention.

The present invention relates to methods and apparatus for integrating one-way and
 10 two-way security systems to enable secure distribution of services. As shown in Figure 1, a decryption device 110 is provided which is enabled to securely receive and decrypt encrypted services 120 from one or more service providers 150. A consumer device 100 is provided which is enabled to securely communicate with the decryption device 110. A user interface 130 associated with the consumer device 100 is provided for initiating a service
 15 request 140 for a requested service 135 from the one or more service providers. In operation, the service request 140 is communicated from the consumer device 100 to the decryption device 110. The requested service is then acquired by the decryption device 110 from the one or more service providers in response to the service request as an encrypted requested service 120. The acquired encrypted requested service 120 is then decrypted by
 20 the decryption device 110. The requested service is re-encrypted and securely communicated from the decryption device 110 to the consumer device 100 (e.g., as re-encrypted service 105). The re-encrypted requested service 105 can then be decrypted and decoded at the consumer device 100 to provide the requested service 135.

The service request 140 may be communicated from the consumer device 100 to
 25 the decryption device 110 via one of a secure channel or a non-secure channel.

The requested service 135 may be securely acquired by the decryption device 110 from the service provider 150. The requested service 135 may be received by the decryption device in an encrypted multiplex of services (e.g., encrypted services 120). If so, the decryption device 110 may be adapted to decrypt the multiplex of services 120 in
 30 order to acquire the requested service 135.

The received encrypted services 120 may be received in a first encryption format and the re-encrypted requested service 105 may be encrypted in a second encryption format compatible with the consumer device 100.

5 The consumer device 100 may establish a secure socket layer (SSL) connection with the decryption device 110. The SSL connection may be enabled via one of a Transmission Control Protocol/Internet Protocol (TCP/IP) transport scheme, an MPEG-2 transport scheme, or any other type of transport scheme, including a proprietary transport scheme. The service request 140 may be securely communicated from the consumer device 100 to the decryption device 110 via the SSL connection.

10 The requested service 135 may be a parentally controlled service. In such an embodiment, the decryption device 110 may communicate a response to the consumer device 100 requesting access information for the parental controlled service. The access information may be provided by a user via the user interface 130. The access information may be securely communicated from the consumer device 100 to the decryption device 15 110. In the event the access information is verified by the decryption device 110, the user is authorized to receive the requested service 135. The access information may comprise at least one of a personal identification number, a user name, a password, or similar access control information.

The requested service 135 may be a pay-per-view service. The decryption device 20 110 may communicate a response to the consumer device 100 requesting payment or authorization information for the pay-per-view service. The payment or authorization information may be provided by a user via the user interface 130. The payment or authorization information may be securely communicated from the consumer device 100 to the decryption device 110. In the event the payment or authorization information is verified 25 by the decryption device 110, the user is authorized to receive the requested pay-per-view service.

A smart card interface may be provided to enable the payment or authorization for the requested pay-per-view service. The smart card interface may be integrated into or part of the user interface 130, the consumer device 100, or the decryption device 110.

30 The consumer device 100 may comprise an Internet appliance, a personal computer, a personal digital assistant, a cellular telephone, or the like. The decryption device 110 may comprise a digital television terminal, a digital television, or the like. The user interface 130 may comprise one of an interactive display device, a remote control

device adapted for communication with the consumer device, a touch screen associated with the consumer device, a joystick associated with the consumer device, a mouse, a touch pad associated with the consumer device, or any other similar type of interface.

In an example embodiment of the invention as shown in Figure 2, the decryption
5 device 110 may comprise a first secure socket layer (SSL) processor 210 for enabling SSL communications and re-encrypting the requested service. A service selector 240 for acquiring the requested service (as an encrypted requested service 120) from the one or more service providers, in response to the service request 250, may also be provided as part of the decryption device 110. A decryption processor 215 in the decryption device 110 may
10 be provided for decrypting the encrypted services 120 received from the one or more service providers.

The service request may be received by the SSL processor 210 and forwarded from the SSL processor to the service selector 240. The service selector 240 may acquire the requested service from the one or more service providers as an encrypted requested service
15 120. The decryption processor 215 may then decrypt the encrypted requested service 120, providing decrypted requested service 230 to the service selector 240. The service selector 240 forwards the decrypted requested service to the SSL processor 210 as requested service 245. The SSL processor 210 re-encrypts the requested service 245 as an SSL encrypted service 225. The SSL encrypted service 225 is securely communicated from the
20 decryption device 110 to the consumer device 100 (e.g., via data transport mechanism 205) as SSL encrypted service 105, where it can be decrypted.

The service selector 240 may acquire the requested service using standard service acquisition mechanisms. For example, a service identifier (e.g., a channel map number from a channel map) may be passed to the service selector 240 via a software API call
25 (e.g., from processor 210). The service selector 240 then initiates a tuning operation to tune a tuner (not shown) to a specific frequency. In the case of digital services, the service selector 240 also handles signal (e.g., quadrature amplitude modulation (QAM)) lock, program table acquisition filtering, and ultimately service selection from the multiplex of services received.

30 As shown in Figure 3, the consumer device 100 may comprise a second SSL processor 310 for decrypting the re-encrypted service 315 and a decoder 340 for decoding the decrypted (i.e., unencrypted) requested service 355. A service request handler 330 receives the service request 140 from the user interface 130. The service request 350 is

forwarded from the service request handler 330 to the second SSL processor 310. The second SSL processor 310 forwards the service request 335 on to the decryption device 110 via the data transport mechanism 305. The service request may then be processed by the decryption device 110 as discussed above in connection with Figure 2. The SSL encrypted service 105 may be received by the consumer device 100 from the decryption device 110 at data transport mechanism 305, which forwards SSL control data 320 and SSL encrypted service 315 to SSL processor 310. The second SSL Processor 310 can then decrypt the SSL encrypted services 315 and forward the decrypted (unencrypted) service 355 to decoder 340 for decoding. The decoded service 135 can then be output for display.

In a further example embodiment, the decryption device 110 may be located at a television headend. In such an embodiment, the consumer device 100 may comprise a digital television terminal. The decryption device 110 may decrypt services received in a first encryption format and re-encrypt a requested service in a second encryption format for communication to the digital television terminal 100. The first encryption format may comprise secure socket layer (SSL) encryption. The second encryption format may comprise an encryption format compatible with a television system network distribution system.

The decryption device 110 may include multiple decryption processors 215 for decrypting multiple services received from multiple service providers 150. The decryption device 110 is enabled to process multiple service requests received simultaneously from multiple digital consumer devices 100.

The consumer device 100 may be one of a plurality of consumer devices in a television system network. The decryption device 110 may be a digital television terminal in a television system network. The consumer device 100 may be enabled to securely access the decryption device 110 from a remote location. For example, the consumer device 100 may securely access the decryption device 110 via a broadband connection from the remote location.

The encrypted services 120 may comprise one of pay-per-view services, television programs, Internet content, streaming media content, audio content, video content, audiovisual content, or the like.

The service providers 150 may comprise at least one of an Internet provider, a telephone provider, a cable television provider, a satellite television provider, an off-air television provider, a streaming media provider, or a radio station.

The decryption device 110 may be located within a local network. Multiple consumer devices 100 within the network may be enabled to securely communicate with the decryption device 110. The decryption device 110 may comprise a plurality of decryption processors 215 for decrypting multiple services in response to a multiple service requests. The decryption device 110 may comprise a digital television terminal. The multiple consumer devices 100 may each comprise one of a personal computer, an Internet appliance, a personal digital assistant, a cellular telephone, or the like. The decryption device 110 may comprise one of a secure broadband gateway (SBG) or a secure broadband modem (SBM).

The re-encrypted requested service may be decrypted and decoded at the decryption device 110 and then output from the decryption device 110, rather than or in addition to being passed on to the consumer device 100. For example, the decryption device 110 may be a television terminal and the consumer device 100 may comprise an Internet appliance. In addition to enabling secure communications of the service from the television terminal to the Internet appliance, the television terminal is enabled to decrypt the re-encrypted services and decode them for display on the television. Alternatively, a separate path may be provided which enables the television terminal to decrypt and decode the service as originally received for display on the television (i.e. without the need to re-encrypt and then decrypt again).

The present invention may be used, for example, to enable the secure distribution of video and/or audio services from consumers' homes to remote locations. As one example, a consumer may purchase a service from a television provider for a digital video recorder enabled television "set-top" terminal. The consumer, while traveling, could login to the terminal from a laptop using a broadband connection and securely stream content that has been recorded on the terminal to their remote laptop. Various other uses for the present invention will be apparent from those skilled in the art from the disclosure above.

It should now be appreciated that the present invention provides advantageous methods and apparatus for integrating one-way and two-way security systems, such as consumer devices and decryption devices, to enable increased distribution of services in a secure manner.

The scope of the claims should not be limited by the preferred embodiments set forth in the examples, but should be given the broadest interpretation consistent with the description as a whole.

What is claimed is:

1. Apparatus for integrating one-way and two-way security systems to enable secure distribution of services, comprising:

a decryption device enabled to securely receive and decrypt encrypted services from one or more service providers;

a consumer device enabled to securely communicate with said decryption device;

a user interface associated with said consumer device for initiating a service request for a requested service from said one or more service providers;

wherein:

said service request is communicated from said consumer device to said decryption device;

said requested service is acquired by said decryption device from said one or more service providers in response to said service request as an encrypted requested service;

the acquired encrypted requested service is decrypted by said decryption device;

said requested service is re-encrypted and securely communicated from said decryption device to said consumer device; and

said re-encrypted requested service is decrypted and decoded at said consumer device to provide said requested service, wherein said decryption device comprises:

a first secure socket layer (SSL) processor for enabling SSL communications and re-encrypting said requested service as an SSL encrypted service;

a service selector for acquiring the requested service from said one or more service providers in response to said service request as an encrypted requested service; and

a decryption processor for decrypting said encrypted services received from said one or more service providers.

2. Apparatus in accordance with claim 1, wherein said service request is communicated via one of a secure channel or a non-secure channel.

3. Apparatus in accordance with claim 1, wherein said requested service is securely acquired by said decryption device.

4. Apparatus in accordance with claim 1, wherein:

said requested service is received by said decryption device in an encrypted multiplex of services; and

said decryption device decrypts said multiplex in order to acquire said requested service.

5. Apparatus in accordance with claim 1, wherein:

said received encrypted services are received in a first encryption format; and

said re-encrypted requested service is encrypted in a second encryption format compatible with said consumer device.

6. Apparatus in accordance with claim 1, wherein:

said decryption device is located within a local network; and

multiple consumer devices within said network are enabled to securely communicate with said decryption device.

7. Apparatus in accordance with claim 1, wherein:

said re-encrypted requested service is decrypted and decoded at said decryption device; and

said requested service is output from said decryption device.

8. A method for integrating one-way and two-way security systems to enable secure distribution of services, comprising:

initiating a service request for a requested service on a consumer device via a user interface;

communicating said service request from said consumer device to a decryption device;

enabling said requested service to be acquired by said decryption device as an encrypted requested service in response to said service request;

decrypting the acquired encrypted requested service at said decryption device;

re-encrypting said requested service at said decryption device;

securely communicating said requested service from said decryption device to said consumer device; and

decrypting and decoding said re-encrypted requested service at said consumer device to provide said requested service, wherein said decryption device comprises:

a first secure socket layer (SSL) processor for enabling SSL communications and re-encrypting said requested service as an SSL encrypted service;

a service selector for acquiring the requested service from said one or more service providers in response to said service request as an encrypted requested service; and

a decryption processor for decrypting said encrypted services received from said one or more service providers.

9. A method in accordance with claim 8, wherein said service request is communicated via one of a secure channel or a non-secure channel.

10. A method in accordance with claim 8, wherein said requested service is securely acquired by said decryption device.

11. A method in accordance with claim 8, wherein:

said requested service is received by said decryption device in an encrypted multiplex of services; and

said decryption device decrypts said multiplex in order to acquire said requested service.

12. A method in accordance with claim 8, wherein:

said received encrypted services are received in a first encryption format; and

said re-encrypted requested service is encrypted in a second encryption format compatible with said consumer device.

13. A method in accordance with claim 8, wherein:

said decryption device is located within a local network; and
multiple consumer devices within said network are enabled to securely communicate with said decryption device.

14. A method in accordance with claim 8, wherein:

said re-encrypted requested service is decrypted and decoded at said decryption device; and
said requested service is output from said decryption device.

15. A decryption device comprising:

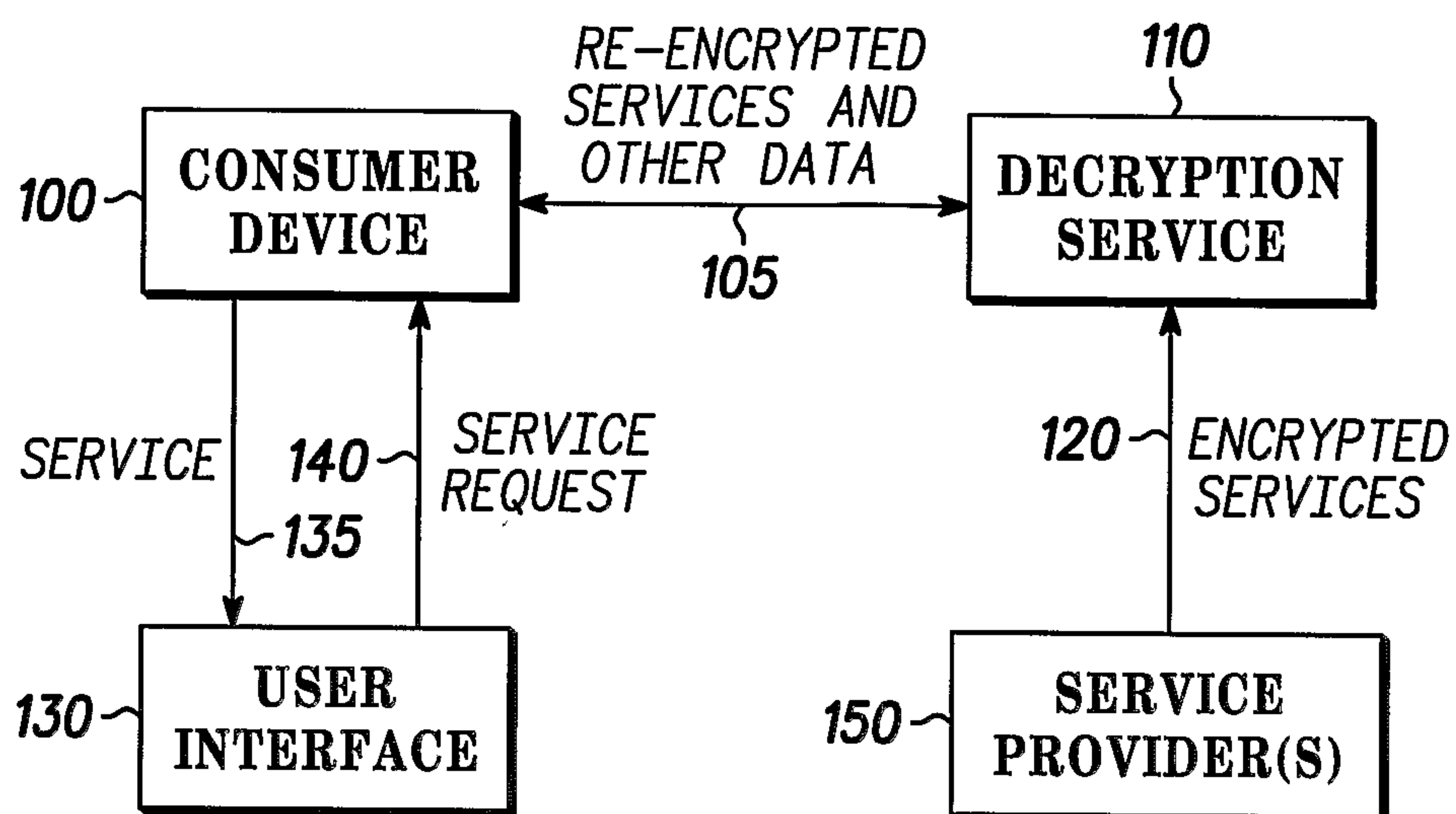
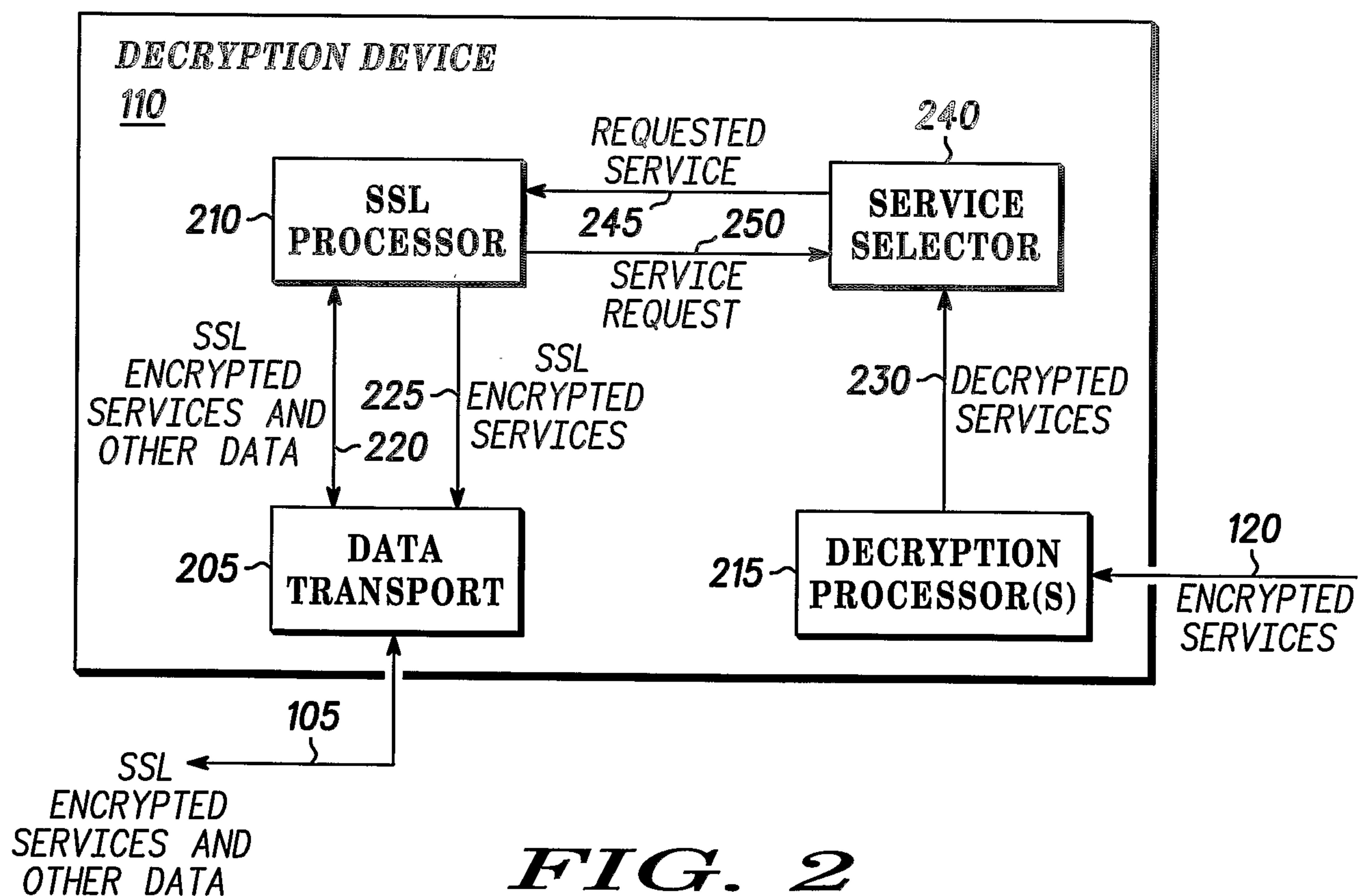
a service selector enabled to acquire an encrypted requested service from one or more service providers in response to a service request received from a consumer device;
a decryption processor enabled to decrypt the encrypted requested service; and
a secure socket layer (SSL) processor enabled for (i) providing SSL communications with the consumer device; and (ii) re-encrypting the requested service for secure communication to the consumer device as an SSL encrypted service.

16. A consumer device comprising:

a secure socket layer (SSL) processor enabled for providing SSL communications with an encryption device and decrypting re-encrypted services received from said encryption device; and
a decoder enabled to decode said decrypted requested service;
wherein:
said consumer device is enabled to communicate a service request to the decryption device for a requested service;

said requested service is acquired by said decryption device from one or more service providers in response to said service request as an encrypted requested service; the acquired encrypted requested service is decrypted by said decryption device; and said requested service is re-encrypted and securely communicated from said decryption device to said consumer device as an SSL encrypted service.

1/2

*FIG. 1**FIG. 2*

2/2

