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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2438357 A1 2005/02/26

(21) 2 438 357

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2003/08/26

(41) Mise à la disp. pub./Open to Public Insp.: 2005/02/26

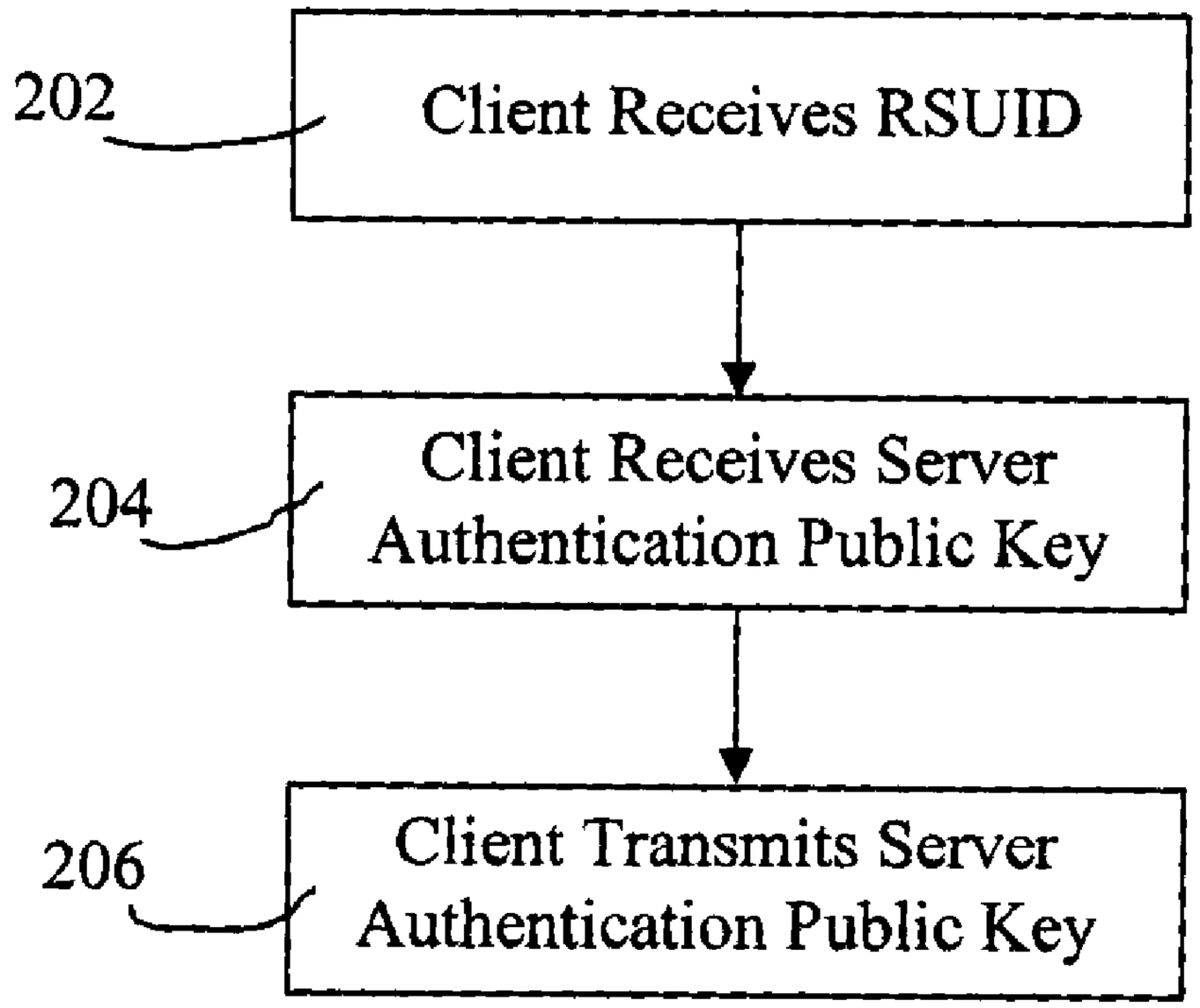
(51) Cl.Int.^{7}/Int.Cl.^{7} H04L 12/22, H04L 9/32

(71) Demandeur/Applicant:
IBM CANADA LIMITED - IBM CANADA LIMITEE, CA

(72) Inventeurs/Inventors:
WILDING, MARK F., CA;
HORMAN, RANDALL W., CA

(74) Agent: ROSEN, ARNOLD

(54) Titre : SYSTEME ET METHODE D'ACCES A DISTANCE SECURISE
(54) Title: SYSTEM AND METHOD FOR SECURE REMOTE ACCESS



(57) Abrégé/Abstract:
Disclosed is a method of directing a client to establish a secure connection with a server across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process. The method includes the steps of: transmitting to the server a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key, receiving from the server a server information package having the RSUID and a server challenge information package and a portion of the received client challenge information encrypted with the Client Authentication Public Key, using the Client Authentication Private Key to decrypt and verify the server challenge information package, and, transmitting to the server an encrypted portion of the received client challenge information.

ABSTRACT

Disclosed is a method of directing a client to establish a secure connection with a server across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process. The method includes the steps of: transmitting to the server a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key, receiving from the server a server information package having the RSUID and a server challenge information package and a portion of the received client challenge information encrypted with the Client Authentication Public Key, using the Client Authentication Private Key to decrypt and verify the server challenge information package, and, transmitting to the server an encrypted portion of the received client challenge information.

SYSTEM AND METHOD FOR SECURE REMOTE ACCESS

FIELD OF THE INVENTION

[0001] The present invention relates generally to a system and method for establishing a secure connection between a server and a client over a public network and specifically to a method for providing secure remote access to the client by the server.

BACKGROUND

[0002] Referring to Figure 1, a system for a remote software product environment is illustrated generally by numeral 100. The system 100 includes a customer system 102 and a service organization system 104. The customer system 102 includes a software product 106 and a service client 108. The service organization 104 includes a service gateway 110 and a session end point 112. The service client 108 is coupled with the service gateway 110 via a network 114. Typically, the network 114 is a public network, such as the Internet. Optionally, one or both of the service client 108 and the service gateway 110 are connected to the network 114 via a firewall 116.

[0003] Servicing a remote software product has many challenges, including transferring diagnostic data from the customer system 102 to the organization system 104, transferring software product updates from to the organization system 104 to the customer system 102, and remote troubleshooting for problem diagnosis.

[0004] Transferring diagnostic data from the customers system 102 to the organization system 104 is an issue since diagnostic data often contains sensitive information. Typically, a File Transfer Protocol (FTP) is used for transferring files, even though it is inconvenient for the customers and insecure for both the customers and the service organization.

[0005] Transferring software product updates, such as fixpaks and service releases to customer system 102 from the organization system 104 is an issue since the organization system 104 providing the latest software product update should be authenticated to ensure that a malicious server is not providing malicious software instead of the expected software product update. Typically, certificates issued by a trusted third party are used for authenticating the organization system 104.

[0006] Yet further, the need for remote troubleshooting between the customer system 102 and the organization system 104 provides several issues. For example, telephone support is typically provided by many organizations. Telephone conversations can easily lead to lost information and many errors are difficult to communicate over the telephone. Alternately, some customers will allow a telnet connection into their customer system 102, which is very insecure.

[0007] Today, there is no convenient and secure facility that can alleviate these challenges. As software and hardware products become more complex, the need for convenient and a secure remote service facility is becoming more and more critical. In fact, such a solution is already desperately required. As a result, it is an abject of the present invention to obviate or mitigate at least some of the above mentioned disadvantages.

SUMMARY

[0008] In accordance with an aspect of the present invention there is provided a method of directing a client to establish a secure connection with a server across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the method including: transmitting to the server a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key, receiving from the server a server information package having the RSUID and a server challenge information package and a portion of the received client challenge information encrypted with the Client Authentication Public Key, using the Client Authentication Private Key to decrypt and verify the server challenge information package, and, transmitting to the server an encrypted portion of the received client challenge information.

[0009] In accordance with another aspect of the invention, there is provided a computer program product having a computer readable medium tangibly embodying computer executable code for directing a client to establish a secure connection with a server across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the computer program product including code for directing the client to: transmit to the server a client information package having the RSUID and a client challenge

information package encrypted with the Server Authentication Public Key, receive from the server a server information package having the RSUID and a server challenge information package and a portion of the received client challenge information encrypted with the Client Authentication Public Key, use the Client Authentication Private Key to decrypt and verify the server challenge information package, and, transmit to the server an encrypted portion of the received client challenge information.

[0010] In accordance with yet another aspect of the invention, there is provided a method for directing a server to establish a secure connection with a client across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the method including: receiving from the client a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key, using the RSUID to retrieve an associated Server Authentication Private Key, using the Server Authentication Private Key to decrypt and verify the client challenge information package, and, transmitting to the client a server information package having the RSUID and a server challenge information package encrypted with the Client Authentication Public Key.

[0011] In accordance with yet another aspect of the invention, there is provided a computer program product having a computer readable medium tangibly embodying computer executable code for directing a server to establish a secure connection with a client across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the computer program product including code for directing the server to: receive from the client a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key, use the RSUID to retrieve an associated Server Authentication Private Key, use the Server Authentication Private Key to decrypt and verify the client challenge information package, and, transmit to the client a server information package having the RSUID and a server challenge information package encrypted with the Client Authentication Public Key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The embodiments of the present invention will be explained by way of the following drawings, in which:

Figure 1 is block diagram of a remote software product environment (prior art);

Figure 2 is a flow chart illustrating the operation of a registration process in accordance with an embodiment of the invention; and

Figures 3A and 3B are a flow chart illustrating the operation of establishing a secure session between a server and a client in accordance with an embodiment of the invention.

[0013] Similar references are used in different figures to denote similar components.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] The following detailed description of the embodiments of the present invention does not limit the implementation of the invention to any particular computer programming language. The present invention may be implemented in any computer programming language provided that the Operating System (OS) provides the facilities that may support the requirements of the present invention. A preferred embodiment is implemented in the C or C++ computer programming language (or other computer programming languages in conjunction with C/C++). Any limitations presented would be a result of a particular type of operating system, computer system, or computer programming language and would not be a limitation of the present invention.

[0015] As previously described, many of the problems relating to servicing a remote software product stem from security related issues associated with communicating remotely through the Internet. These problems relate to connection establishment, authentication, and privacy.

[0016] Since it is often convenient to use the Internet to communicate between the customer system 102 and the organization system 104, the present embodiment of the invention uses an Internet connection for communicating between the two systems. However, any system that allows incoming connections to the Internet is at risk for Denial of Service (DOS) attacks or being compromised by hackers. As a result, most customers do not want a server that accepts

connections on the Internet that could potentially expose their system(s) to the raw internet. Most customers feel reasonably safe about initiating a connecting out to a server on the Internet.

[0017] Further, the invention may have access to potentially damaging functionality or sensitive data. Thus, ensuring that only authorized remote service teams at the service organization 104 have access to the customer system 102 is critical. Likewise, ensuring that only authenticated service clients 108 at the customer system 104 can connect to the service gateway 110 is equally important.

[0018] Yet further, any sensitive data that flows over the public network should be encrypted to prevent a third party from eavesdropping.

[0019] In accordance with the above requirements, the invention enables the customer system 102 to establish a connection with the organization system 104 using a public network, such as the Internet. Further, the invention allows the customer system 102 to communicate with the organization system 104 in a secure manner, while authenticating the identity of the customer system 102 to the organization system 104 and vice versa. Details of the operation of the invention are described as follows.

[0020] Without an extremely high level of security, any remote service facility will put both the service organization system's company and its customers at risk. An initial handshake between the service clients 108 and service gateway 110 is performed for ensuring a high level of security and authentication.

[0021] Initially, a registration process is performed for registering a customer for remote service. Referring to Figure 2, a flow chart illustrating the operation of the registration process is shown. In step 202, the customer receives a Remote Service Unique Identifier (RSUID) that is used to differentiate the customer from other remote service customers. The RSUID need not be confidential and can be shared with the public. In step 204, the customer receives a confidential authentication public key, referred to hereinafter as the Server Authentication Public Key. The Server Authentication Public Key is the public key portion of a public/private key pair generated at the server. The Server Authentication Key is similar to a password in that it is used by the service client 108 for authenticating the service gateway 110. Thus, it is preferable that there is

only one Server Authentication Public/Private Key pair per service client 108. In step 206, the customer generates a public/private key pair. The public key, referred to hereinafter as the Client Authentication Public Key, is provided to the server. Similarly to the Server Authentication Public Key, it is preferable that the Client Authentication Public Key remain unadvertised and confidential.

[0022] The operation described above is typically performed only at registration. However, the customer may request to reregister occasionally for a variety of reasons, such as for a suspected security breach. Thus, it can be seen that the registration process described with reference to Figure 2 will be performed relatively infrequently. As a result, this operation can be performed offline, or using encryption to transfer the data and certificates from a trusted third party to authenticate the customer and server.

[0023] Once the customer has registered with the server, a remote service session can be established. Referring to Figure 3, a flow chart illustrating the steps for establishing a remote session is shown. In step 302, the customer system initiates a connection. The service client 104 establishes a Transmission Control Protocol/ Internet Protocol (TCP/IP) connection, or session, to the service gateway. This is similar to having the customer use the telnet protocol to connect to a remote system through the Internet, although the following steps ensure a much higher level of security than a telnet connection.

[0024] In step 304, the service gateway 110 generates a Temporary Server Public/Private key pair. The Temporary Server Public Key is transmitted, unencrypted, to the service client 108 for use in initiating the session.

[0025] In step 306, the service client 104 encrypts a client challenge information package using the Server Authentication Public Key, received from the service client at step 204 of the registration operation. The client challenge information package includes the following components. A session counter identifying the number of times that a service session has been established for this particular Remote Service Unique Identifier. A Client Session Public Key that it wishes to use for this session. Alternately, instead of the Client Session Public Key, a previous session ID can be included. A word length value representing the length of a Server Challenge Word. Preferably, the length is between 64 and 256 bytes. The Server Challenge

Word comprises a random number of randomly generated bytes of information, generated by the service client 108. A flag value, typically an integer, contains a set of flags, which request the type of session to establish, such as unidirectional, bidirectional, and the like. Optionally, the client challenge information package may include a session indicator for identifying the session lifetime.

[0026] In step 307, the service client 108 uses the Temporary Server Public Key to encrypt a client identification information package. Preferably, the client identification information package is independent of the software version of the software product 106. Further, the client identification information package includes the Remote Service Unique Identifier and the encrypted client challenge information package.

[0027] In step 308, the service client 108 sends the client identification information package to the service gateway 110. In step 309, the service gateway 110 uses the Temporary Server Private Key to decrypt the client identification information package. The Remote Service Unique Identifier is used to look up a corresponding Server Authentication Private Key, which is used to attempt to decrypt the client challenge information package.

[0028] In step 310, it is determined whether the service gateway 110 can decrypt the client challenge information package. That is, if the service gateway 110 can interpret and verify the client challenge information package, the service client 108 will have been authenticated and the service gateway 110 proceeds to step 314. If the service gateway 110 cannot decrypt the client challenge information it proceeds to step 312.

[0029] In step 312, the service gateway 110 sends an error message to the service client 108 and immediately closes the connection. Closing the connection immediately is important to reduce the impact of Denial of Service attacks that are TCP/IP connection establishment related.

[0030] In step 314, the service gateway 110 uses the Client Authentication Public Key, received from the service client at step 206 of the registration operation, for encrypting a server challenge information package. The server challenge information package includes the following components. A number of times that a service session has been established for this Remote Unique Service Identifier. A Server Session Public Key that the service gateway wishes to use

for the duration of the session. Alternately, instead of the Client Session Public Key, a previous session ID can be included. The Server Challenge Word is returned to prove that the service gateway could decrypt the client challenge information package. A confirmation flag value, typically an integer, that contains a set of flags confirming the type of session to establish. A large, for example 256-byte, randomly generated Client Challenge Word and a session identification (ID). Optionally, the server challenge information package may include a session indicator for confirming the session lifetime.

[0031] In step 316, the service gateway 110 uses the Client Session Public Key received from the service client 108 in the client identification information package to encrypt a server identification information package. If the client identification information package included a session ID instead of a Client Session Public Key, the Client Session Public Key associated with the session ID is used to encrypt the server identification information package. The server identification information package includes the Remote Service Unique Identifier and the server challenge information package. In step 318, the service gateway 110 sends the server identification information package to the service client 108.

[0032] In step 320, the service client 108 uses the Client Session Private Key to decrypt the server identification information package and the Client Authentication Private Key to attempt to decrypt the server challenge information package.

[0033] In step 322, it is determined whether the service client 108 can decrypt the server challenge information package. That is, if the service client 108 can interpret and verify the server challenge information package, the service gateway 110 will have been authenticated and the service client 108 proceeds to step 326. If the service client 108 cannot decrypt the server challenge information it proceeds to step 324.

[0034] In step 324, the service client 108 sends an error message to the service gateway 110 and immediately closes the connection. In step 326, the service client uses the Server Session Public Key received in the server challenge information package to encrypt the received Client Challenge Word and session ID. If the server challenge information includes a previous session ID instead of the Server Session Public Key, a Server Session Public Key associated with the previous session ID is used to encrypt the Client Challenge Word and current session ID. In step

328, the encrypted Client Challenge Word and session ID are transmitted to the service gateway 110 to prove that the service client 108 could decrypt the server challenge information package.

[0035] At this point, a remote, secure, authenticated and encrypted connection has been established between the service client 108 and the service gateway 110. The encryption for the connection is performed using the exchanged sessions keys for both sides, which were encrypted twice before they were transmitted.

[0036] Each newly established session can be uniquely identified by the Remote Service Unique Identifier and the Session ID. When a new session is created, the service gateway 110 sends a notification of the session to a default-session handling facility. The notification includes the Remote Service Unique Identifier, the Session ID, and a newly generated internal session password. The default session-handling facility may be one or more service analysts or it may be an automated service program.

[0037] A session may be transferred between session-handling facilities, where the session-handling facility is handled by a human, computer program, or other handling facility. Further, a session may be transferred between any number of session handling facilities, where the session can be handled by more than one session-handling facility at any given time. Yet further, it is possible that any type of remote service capability or facility can use the secure service session.

[0038] If the session is prematurely broken due to a network error or the like, the session ID can be used to re-establish the connection. Thus, it is preferable that both sides store the session ID, the public key of the remote side and the private key for the local side for a session. A session can only be re-established from the customer's system.

[0039] A customer can register or un-register for remote service at any time, which provides another level of security. For customers who want even more security, they may choose to only register for remote service when a major problem occurs.

[0040] Although the method for creating a secure session described above is described as a single method, it is likely that in practice the method will be implemented as two dependent methods, running independently of each other. The first method comprises the client method, which attempts to validate and connect to a server. The second method comprises the server

method, which attempts to validate and connect to a client. It is possible that an unauthenticated client may try to connect to the server, or that the client may try to connect to an unauthenticated server. However, only when an authenticated client tries to connect to an authenticated server will a secure session be established.

[0041] Though the above embodiments are described primarily with reference to a method aspect of the invention, the invention may be embodied in alternate forms. In an alternative aspect, there is provided a computer program product having a computer-readable medium tangibly embodying computer executable instructions for directing a computer system to implement any method as previously described above. It will be appreciated that the computer program product may be a floppy disk, hard disk or other medium for long term storage of the computer executable instructions.

[0042] In yet an alternative aspect, there is provided an article having a computer-readable signal-bearing medium, and having means in the medium for directing a computer system to implement any method as previously described above. It will be appreciated that a supplier of the compiler may upload the article to a network (such as the Internet) and users may download the article via the network to their respective computer systems.

[0043] It will be appreciated that variations of some elements are possible to adapt the invention for specific conditions or functions. The concepts of the present invention can be further extended to a variety of other applications that are clearly within the scope of this invention. Having thus described the present invention with respect to a preferred embodiment as implemented, it will be apparent to those skilled in the art that many modifications and enhancements are possible to the present invention without departing from the basic concepts as described in the preferred embodiment of the present invention. Therefore, what is intended to be protected by way of letters patent should be limited only by the scope of the following claims.

What is claimed is:

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method of directing a client to establish a secure connection with a server across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the method comprising:

transmitting to the server a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key;

receiving from the server a server information package having the RSUID and a server challenge information package and a portion of the received client challenge information encrypted with the Client Authentication Public Key;

using the Client Authentication Private Key to decrypt and verify the server challenge information package; and,

transmitting to the server an encrypted portion of the received client challenge information.

2. The method of claim 1, wherein the client information package is encrypted using a temporary public key assigned by the server.

3. The method of claim 1, wherein the server information package is decrypted using a Client Session Private Key.

4. The method of claim 1, wherein the client challenge information package further includes the Client Session Public Key.

5. The method of claim 1, wherein the client challenge information package further includes a previous session ID for enabling the server to select a Client Session Public Key associated with the previous session ID.

6. A computer program product having a computer readable medium tangibly embodying computer executable code for directing a client to establish a secure connection with a server across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the computer program product comprising code for directing the client to:

transmit to the server a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key;

receive from the server a server information package having the RSUID and a server challenge information package and a portion of the received client challenge information encrypted with the Client Authentication Public Key;

use the Client Authentication Private Key to decrypt and verify the server challenge information package; and,

transmit to the server an encrypted portion of the received client challenge information.

7. The computer program product of claim 6, further including code for encrypting the client information package using a temporary public key assigned by the server.

8. The computer program product of claim 6, further including code for decrypting the server information package using a Client Session Private Key.

9 The computer program product of claim 6, wherein the client challenge information package further includes the Client Session Public Key.

10. The computer program product of claim 6, wherein the client challenge information package further includes a previous session ID for enabling the server to select a Client Session Public Key associated with the previous session ID.

11. A method for directing a server to establish a secure connection with a client across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the method comprising:

receiving from the client a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key;

using the RSUID to retrieve an associated Server Authentication Private Key;

using the Server Authentication Private Key to decrypt and verify the client challenge information package; and,

transmitting to the client a server information package having the RSUID and a server challenge information package encrypted with the Client Authentication Public Key.

12. The method of claim 11, wherein the client information package is decrypted at the server using a temporary private key.

13. The method of claim 11, wherein the server information package is encrypted using a Client Session Public Key.

14. The method of claim 11, wherein the server challenge information package further includes the Server Session Public Key.

15. The method of claim 11, wherein the server challenge information package further includes a previous session ID for enabling the client to select a Server Session Public Key associated with the previous session ID.

16. A computer program product having a computer readable medium tangibly embodying computer executable code for directing a server to establish a secure connection with a client across a public network, the server and the client having exchanged a Server Authentication Public Key, a Client Authentication Public Key, and a Remote Service Unique Identifier (RSUID) during a registration process, the computer program product comprising code for directing the server to:

receive from the client a client information package having the RSUID and a client challenge information package encrypted with the Server Authentication Public Key;

use the RSUID to retrieve an associated Server Authentication Private Key;

use the Server Authentication Private Key to decrypt and verify the client challenge information package; and,

transmit to the client a server information package having the RSUID and a server challenge information package encrypted with the Client Authentication Public Key.

17. The computer program product of claim 16, further including code for decrypting the client information package at the server using a temporary private key.

18. The computer program product of claim 16, further including code for encrypting the server information package using a Client Session Public Key.

19. The computer program product of claim 16, wherein the server challenge information package further includes the Server Session Public Key.

20. The computer program product of claim 16, wherein the server challenge information package further includes a previous session ID for enabling the client to select a Server Session Public Key associated with the previous session ID.

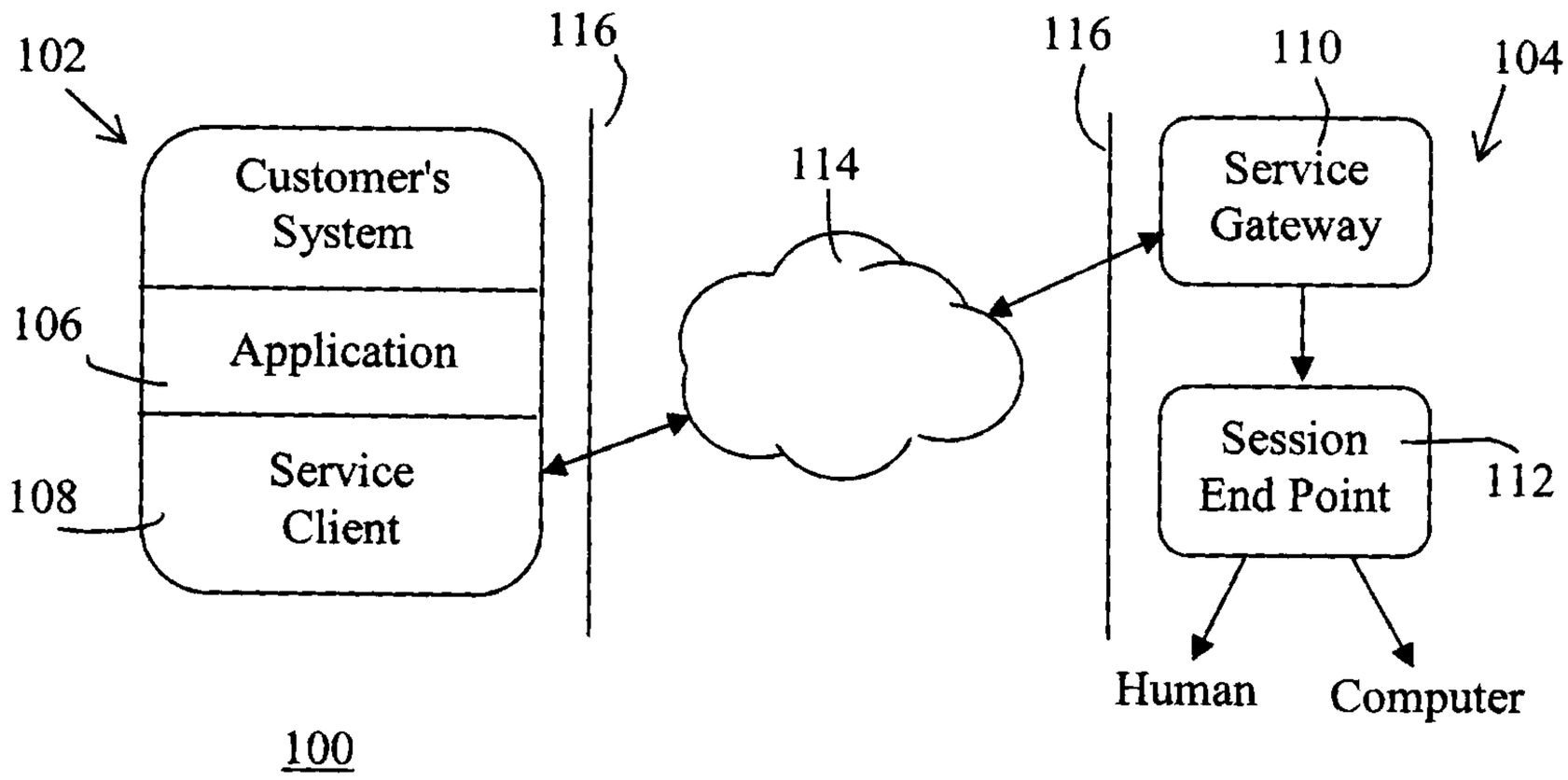


Figure 1

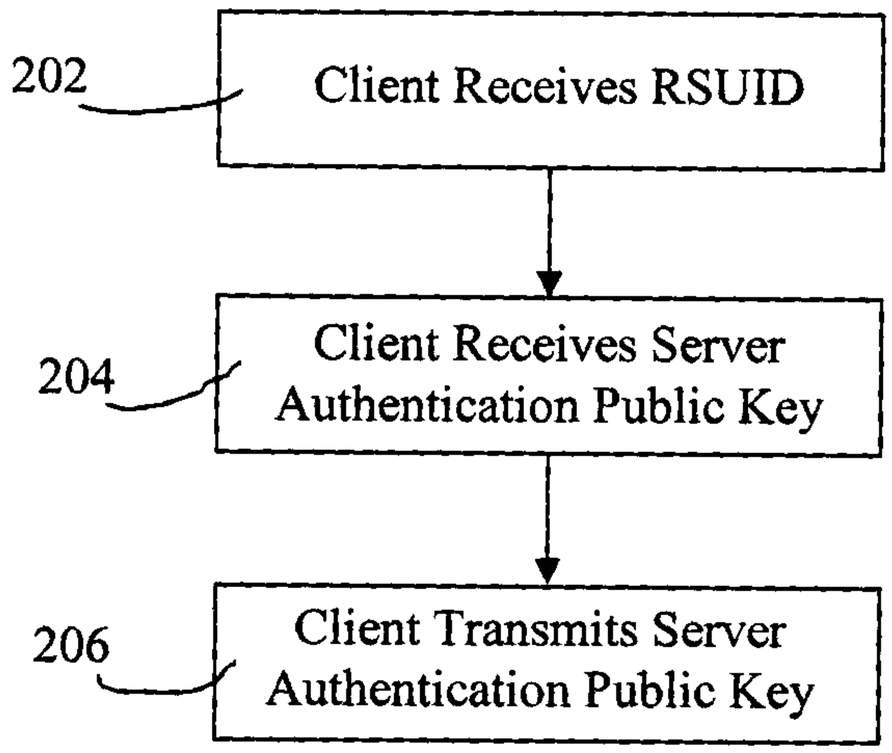


Figure 2

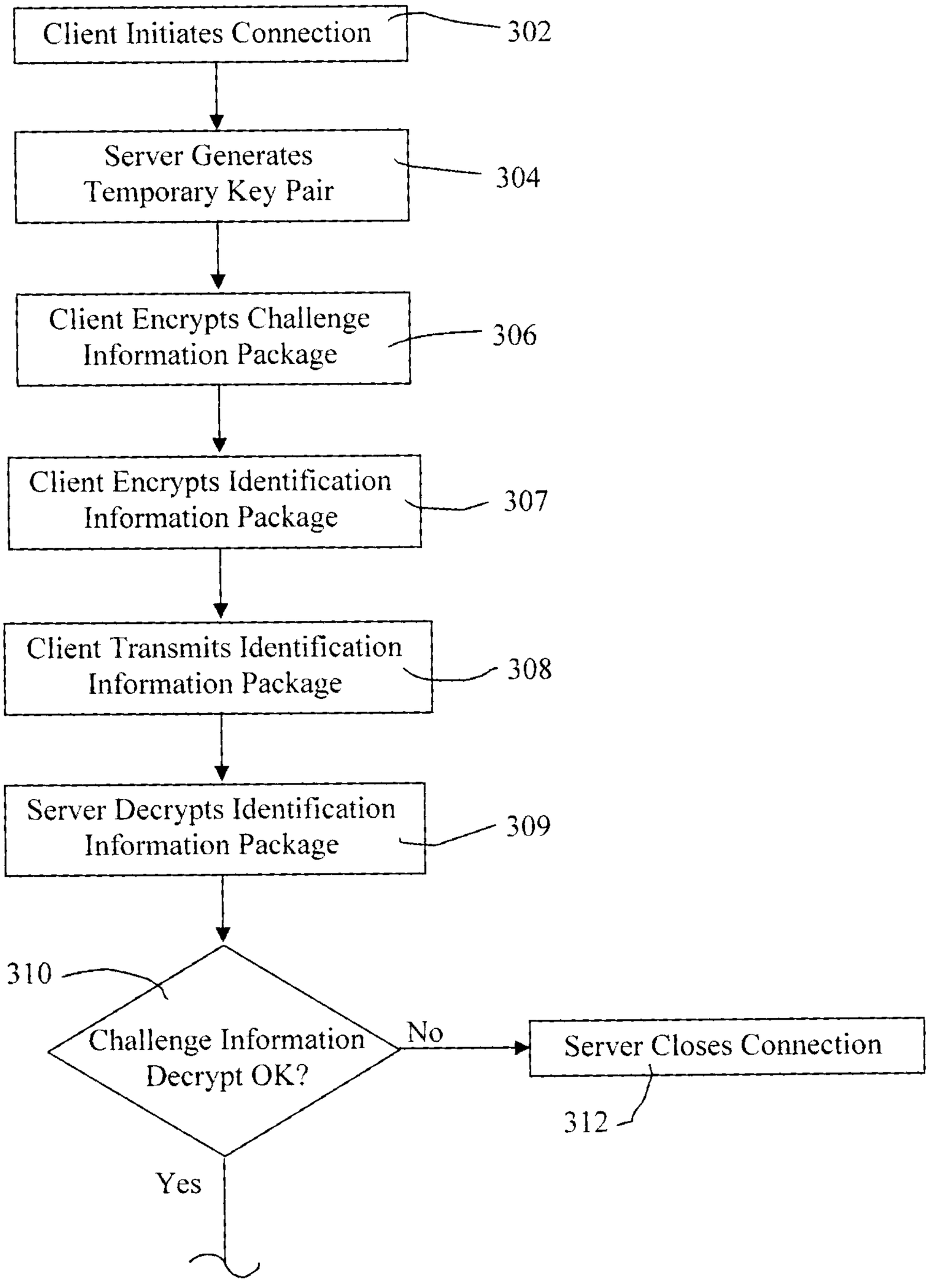

Client Initiates Connection
302
Server Generates Temporary Key Pair
304
Client Encrypts Challenge Information Package
306
Client Encrypts Identification Information Package
307
Client Transmits Identification Information Package
308
Server Decrypts Identification Information Package
309
310
Challenge Information Decrypt OK?
No
Server Closes Connection
312
Yes

Figure 3A

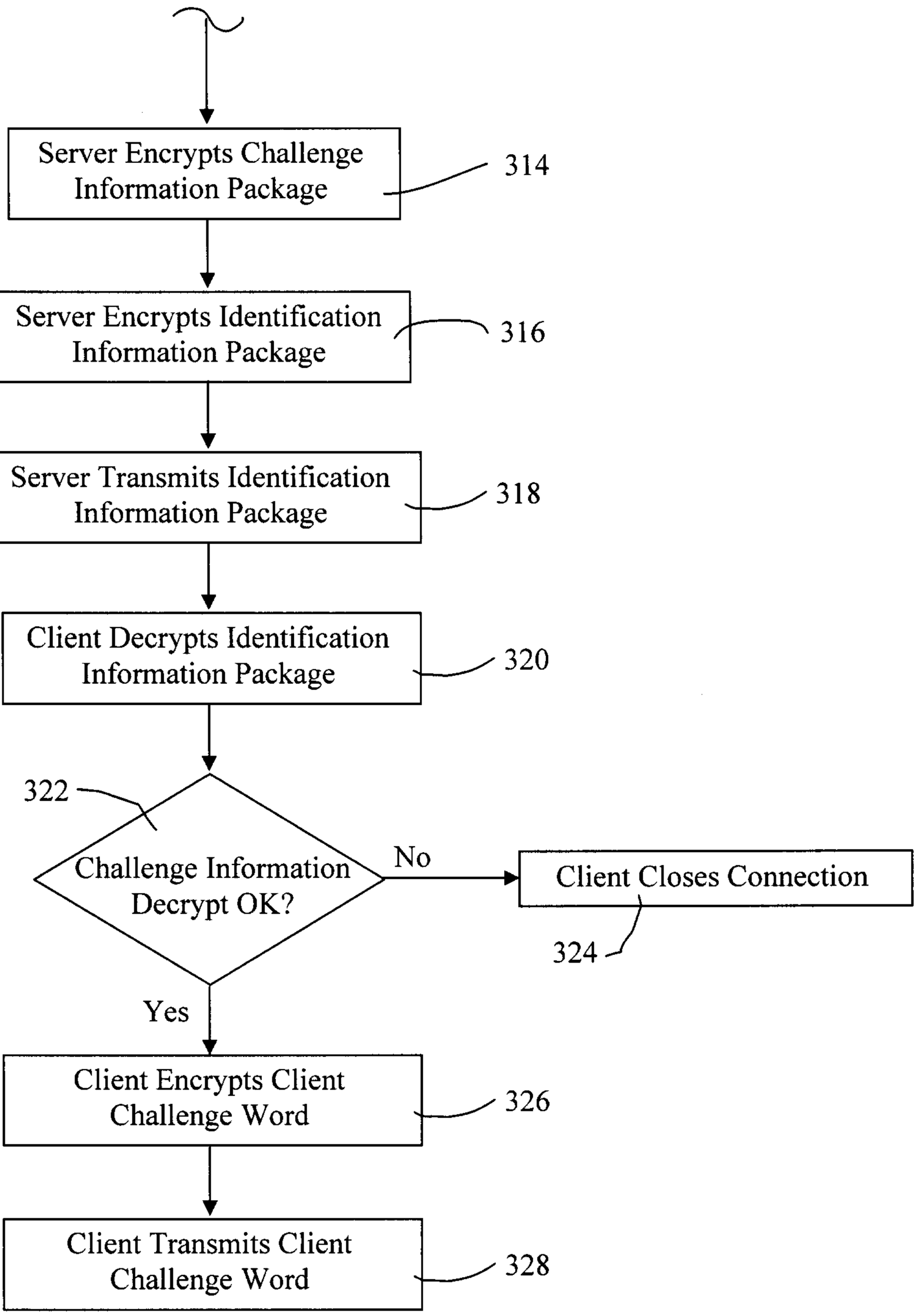
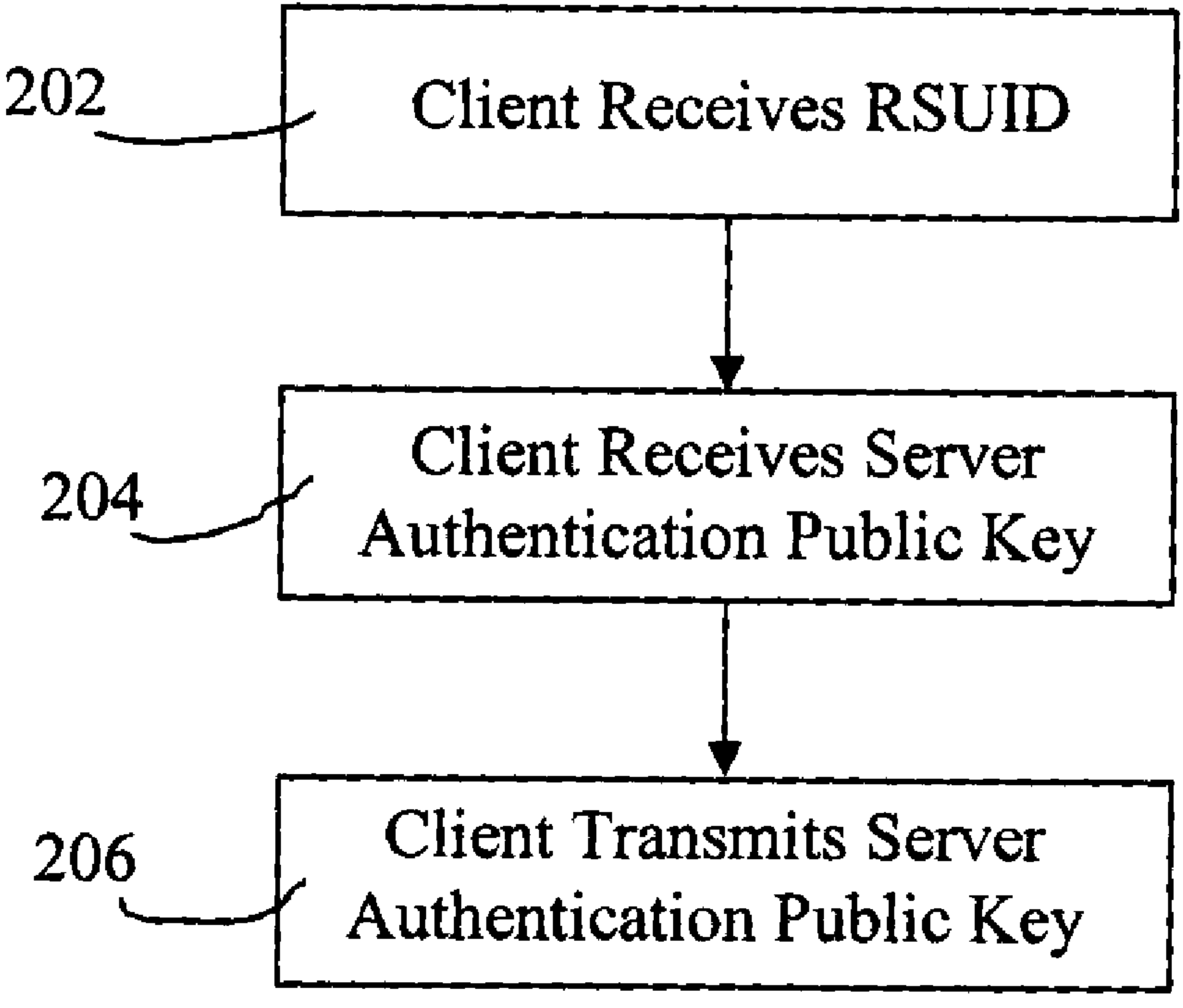

Server Encrypts Challenge Information Package
314
Server Encrypts Identification Information Package
316
Server Transmits Identification Information Package
318
Client Decrypts Identification Information Package
320
322
Challenge Information Decrypt OK?
No
Client Closes Connection
324
Yes
Client Encrypts Client Challenge Word
326
Client Transmits Client Challenge Word
328

Figure 3B


202
Client Receives RSUID
204
Client Receives Server Authentication Public Key
206
Client Transmits Server Authentication Public Key