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

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2527550 A1 2007/05/24

(21) 2 527 550

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(22) Date de dépôt/Filing Date: 2005/11/24

(41) Mise à la disp. pub./Open to Public Insp.: 2007/05/24

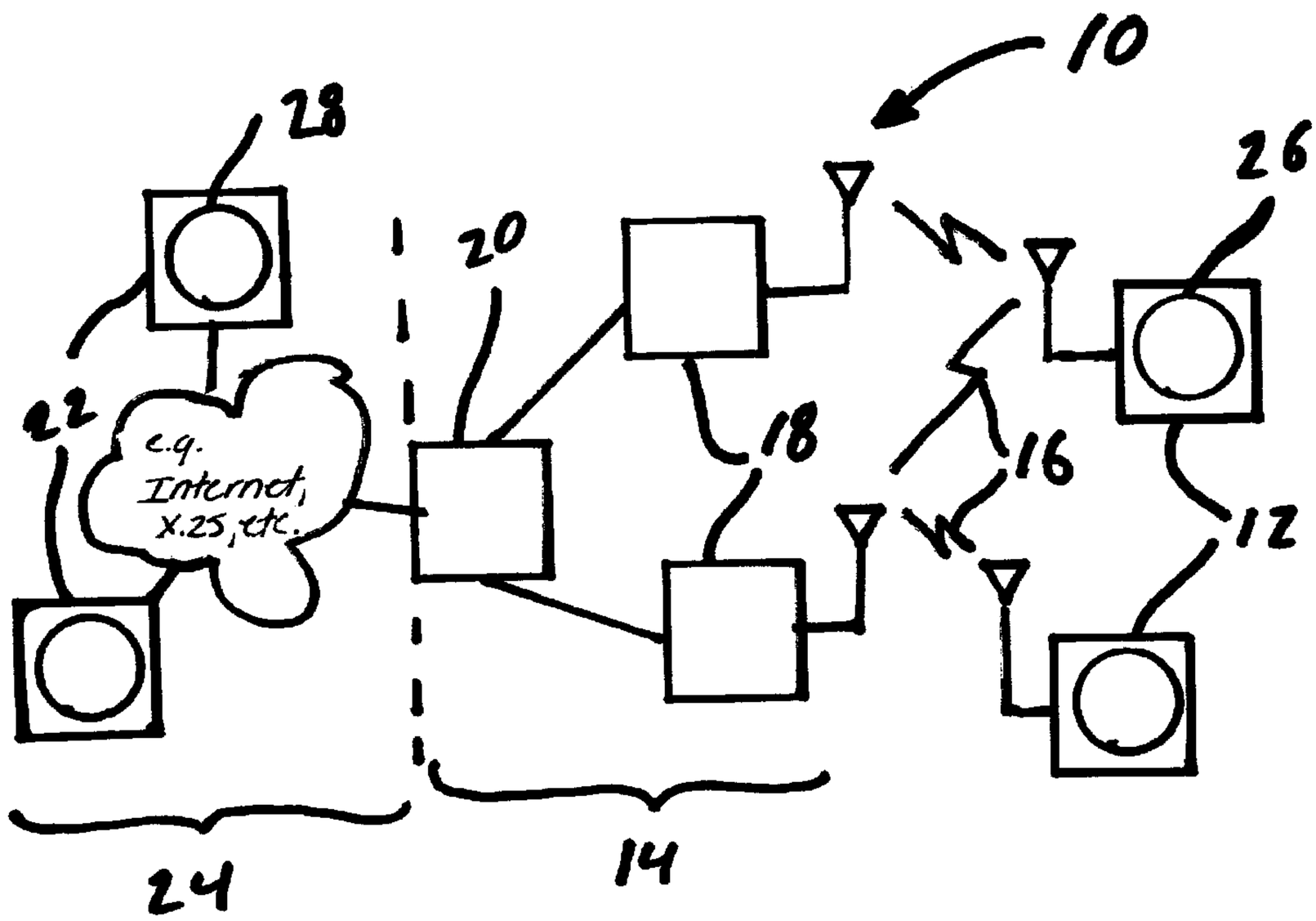
(51) Cl.Int./Int.Cl. *H04L 9/00* (2006.01),
H04L 29/02 (2006.01), *H04Q 7/38* (2006.01)

(71) Demandeur/Applicant:
OZ COMMUNICATIONS, CA

(72) Inventeurs/Inventors:
LEGAULT, SYLVAIN, CA;
THORKELSSON, HARALDUR, CA;
GRIGORIEV, NIKOLAI, CA;
CARON, ALAIN, CA

(74) Agent: GOUDREAU GAGE DUBUC

(54) Titre : METHODE D'ASSOCIATION SURE DE DONNEES A DES SESSIONS HTTPS
(54) Title: METHOD FOR SECURELY ASSOCIATING DATA WITH HTTPS SESSIONS



(57) Abrégé/Abstract:
A method ands system for securely associating external information available at an intermediate node with an HTTPS session. The method comprises the steps of establishing a secure transport between a client and a server, transmitting a secure request from the client to the server via the secure transport using HTTPS, transmitting a secure response from the server to the client via the secure transport using HTTPS, the response comprising an identifier of the intermediate node, a reference to the request and a domain identifier, establishing a first transport between the client and the intermediate node, transmitting a first request from the client to the intermediate node using HTTP, the first request comprising the request reference and the domain identifier, establishing a second transport between the intermediate node and the server, transmitting a second request from the intermediate node to the server using HTTP, the second request comprising the external information, the request reference and the domain identifier, transmitting a first response from the server to the intermediate node and transmitting a second response from the intermediate node to the client.

Abstract

A method ands system for securely associating external information available at an intermediate node with an HTTPS session. The method comprises the steps of establishing a secure transport between a client and a server, transmitting a secure request from the client to the server via the secure transport using HTTPS, transmitting a secure response from the server to the client via the secure transport using HTTPS, the response comprising an identifier of the intermediate node, a reference to the request and a domain identifier, establishing a first transport between the client and the intermediate node, transmitting a first request from the client to the intermediate node using HTTP, the first request comprising the request reference and the domain identifier, establishing a second transport between the intermediate node and the server, transmitting a second request from the intermediate node to the server using HTTP, the second request comprising the external information, the request reference and the domain identifier, transmitting a first response from the server to the intermediate node and transmitting a second response from the intermediate node to the client.

TITLE

METHOD FOR SECURELY ASSOCIATING DATA WITH HTTPS SESSIONS

FIELD OF THE INVENTION

The present invention relates to a method for securely associating data with HTTPS sessions.

BACKGROUND TO THE INVENTION

The prior art reveals providing access to application services, such e-mail and Instant Messaging (IM), from a mobile device such as a mobile telephone. In order to provide access to such applications, the prior art mobile device is equipped with a client which communicates with a server typically via a plurality of communications networks. For example, a mobile core network provides the wireless interconnection between the mobile device and one or more fixed ground stations, or nodes, and an external network, such as the internet, an X.25 network or the like, interconnects the nodes of the mobile core network with the servers of the service provider.

The operator of the core mobile network, typically referred to as a mobile carrier, offers these application services as a "mobile access service" and charges the user of the mobile device for use of such mobile access services. For charging purposes, the mobile carrier requires identification of the user of the mobile access service(s) which is used to identify the mobile user/device but is unrelated to the mobile access service(s) being used.

One example of such an identifier in a GSM network could be the user's unique 16 digit Mobile Station International ISDN Number (MSISDN). The MSISIDN identifier is available from the mobile GSM device whenever the device is communicating with nodes within the mobile core network (e.g. the Home

Location Register, HLR), as it is available at a number of protocol layers. However, when a client resident on the mobile device is communicating with an application located on a server which is outside of the core mobile network, the MSISIDN identifier may be unavailable to the client. This can occur, for instance, when the client comprises a downloadable JAVA midlet or the like, and where for security reasons the JAVA machine in the mobile device does not disclose the MSISDN identifier to JAVA applications.

The prior art reveals a number of methods for providing identification of the mobile device/user. For example, the prior art reveals the client requesting such identification from an intermediate node in the mobile core network and then inserting this identification by the client into the headers of subsequent transmissions. One drawback of this prior art solution is that the client could insert incorrect (and in the worst case fraudulent) identifiers into the headers as there is no way to adequately verify that the source of the identifier is the intermediate node. Additionally, this prior art implementation provides virtually no control over the clients. For example, there is no way to reset identifiers stored on the client side or to force the clients to validate the identifiers.

The prior art also reveals providing a recognizable transaction (packet) format which is then intercepted by an intermediate node and the requisite identifier inserted into the packet. For example, when HTTP is being used for communicating between client and server, intermediate nodes (such as WAP gateways) can add the identifier, or any other information that is not available to the client for that matter, to the HTTP transaction by adding headers to the HTTP request or response.

One drawback of this prior art approach is that it cannot be used when a secure end-to-end tunneling protocol, such as HTTPS, is being used as an intermediate node cannot alter the contents of an HTTPS transaction. Such a secure protocol is needed, for example, when confidential information such a user credentials (User ID and/or password) is to be transmitted.

Another drawback of the above prior art approach is that the intermediate node cannot distinguish between the different types of transactions which are being routed through the node and as a result the identifier must be inserted in all transactions which increases latency and the requisite bandwidth.

SUMMARY OF THE INVENTION

In order to overcome the above and other drawbacks, there is disclosed a method for securely associating external information available at an intermediate node with an HTTPS session. The method comprises the steps of establishing a secure transport between a client and a server, transmitting a secure request from the client to the server via the secure transport using HTTPS, transmitting a secure response from the server to the client via the secure transport using HTTPS, the response comprising an identifier of the intermediate node, a reference to the request and a domain identifier, establishing a first transport between the client and the intermediate node, transmitting a first request from the client to the intermediate node using HTTP, the first request comprising the request reference and the domain identifier, establishing a second transport between the intermediate node and the server, transmitting a second request from the intermediate node to the server using HTTP, the second request comprising the external information, the request reference and the domain identifier, transmitting a first response from the server to the intermediate node and transmitting a second response from the intermediate node to the client.

There is also disclosed a system for securely associating external information available at an intermediate node with an HTTPS session comprising a plurality of clients, at least one intermediate node and at least one. The system implements the above method.

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 is a schematic diagram of a mobile communications network in accordance with an illustrative embodiment of the present invention;

Figure 2 is a diagrammatic representation of the sequence of transactions used to associate data with a connection in accordance with an illustrative embodiment of the present invention;

Figure 3 is a diagrammatic representation of the sequence of transactions used to associate data with a connection in accordance with an alternative illustrative embodiment of the present invention;

Figure 4 is a diagrammatic representation of the sequence of transactions used to associate data with a connection in accordance with a second alternative illustrative embodiment of the present invention; and

Figure 5 is a diagrammatic representation of the sequence of transactions used to associate data with a connection in accordance with a third alternative illustrative embodiment of the present invention.

DETAILED DESCRIPTION OF THE ILLUSTRATIVE EMBODIMENTS

Referring now to Figure 1, a mobile communications network, generally referred to using the reference numeral 10, will now be described. The mobile network 10 is comprised of a number of mobile devices 12 which, for the purposes of transmitting data, communicate with a mobile core network 14 via a wireless connection 16 and one or more ground stations 18. The mobile core network 14 is additionally comprised of one or more intermediate nodes as in 20 (for example, a WAP Gateway or the like) which, amongst other functions, relay data, typically in the form of packets, received from the mobile devices 12

to external devices 22 located on an external network 24, such as the Internet, an X.25 network, or the like.

Each of the mobile devices 12 additionally comprises at least one client 26, such as a JAVA midlet, which communicates with a server application 28 located on the external device 22. The client 26 communicates, or transacts, with the server 28 using a predefined protocol such as TCP/IP, HTTP, HTTPS, or the like.

Referring now to Figure 2 in addition to Figure 1, when a client as in 26 wishes to initiate a transaction which requires a secure transport, an SSL session is established which can subsequently be used by HTTPS for securing communications (typically by requesting a socket connection using TCP/IP and port 443). As known in the art, establishment of an SSL session (tunnel) requires a set of (9) transactions, or messages, to be exchanged between the client 26 and server 28.

Once an SSL session has been established credentials, such as the user ID and password, or other information that must be sent securely, are transmitted from the client 26 to the server 28 over HTTPS. As the request does not include other additional external information that is required by the server 28 in order to proceed (for example an identifier, illustratively the MSISDN, is not present), the server 28 returns a 303 response to the client 26. The server 28 temporarily stores any data that must be processed later.

The 303 response to the client 26 includes a redirection to an intermediate node (such as a WAP gateway or HTTP proxy) as in 20 (which, as will be seen below, will be used to insert an identifier such as the MSISDN into the transaction). This redirect includes a reference to the original request located at the server 28 (for example, using the Application ID and the Session ID). The response also includes at least one cookie (designated in Figures 2 through 5 as Cookie A1 and Cookie A2) to allow the server 28 to verify that subsequent

transactions are related to the initial transaction and are valid for both the secured and unsecured paths. Note that, due to encryption in the SSL connection, the response over HTTPS, including the cookies and any other references, can only be viewed by the client 26, and not by any unauthorized parties.

When the 303 response is received by the client 26, another request is issued by the client 26 which is directed to the intermediate node 20 (for example, a WAP gateway). This transaction does not need to be secured as no confidential information is included (for example, no credentials are transmitted at this point), and can therefore use HTTP. The intermediate node 20 inserts the required information elements into the HTTP header, in particular a mobile device identifier such as the MSISDN. However, if any of the information included by the intermediate node 20 must be transmitted securely, it can optionally be encrypted by the intermediate node 20.

When the server 28 receives the HTTP request with the additional information in the HTTP header, it uses Cookie A1 to ensure that the request is valid and can be associated with the data that was sent over HTTPS. The server 28 may keep the additional information (such as the MSISDN) stored for further transactions by the client 26, or the server 28 may return the additional information encrypted in the response within a cookie to the client 26 (shown in Figures 2 through 5 as Cookie B).

Option "Unsecured Response"

If all subsequent transactions in the session do not require secure transport, the application data response will be returned in the HTTP response. This is shown in Figure 2. After processing the complete request, the server 28 returns 200 OK to the client 26.

Option "Secured Response"

If there is data that must be returned securely to the client, instead of returning 200 OK, the server 28 returns another 303 response to the client 26 to redirect the next request to use HTTPS. Any confidential information can be included in the next response to the client 26. Figure 3 shows a sequence where persistent HTTPS connections are not supported, and the client 26 does not support persistent SSL sessions. After receiving the response to redirect to HTTPS, the client 26 re-establishes SSL with the server 28.

Subsequent requests from the client 26 include both Cookie A2 and Cookie B. Cookie A2 is used to validate that the transactions are from the same source as the original request over HTTPS, and to ensure that requests from unauthorized sources are not processed. This is needed since Cookie B could have been sent or could have been viewed by unauthorized sources. Cookie B contains additional information such as the (e.g. MSISDN) identifier and ensures that the inserted information was from the same originator (for example, to avoid spoofing). Note that the Cookie B may additionally be encrypted so that it may only be read by the server 28.

If the mobile device 12 supports additional capabilities and a secure response from the server 28 is required, some processing and signaling can be eliminated. These sequences are discussed below with reference to Figures 4 and 5.

Figure 4 shows the sequence when the mobile device 12 has the capability to support persistent HTTPS connections, and multiple sockets. One socket is used for HTTPS transactions and another socket is used for HTTP transactions. The sequence of Figure 4 generates less overhead than the sequence of Figure 3, as the SSL session does not need to be re-established.

Figure 5 shows the sequence when the mobile device 12 supports SSL Sessions, but not HTTPS keepalive. In this case, the HTTPS connection must

be re-established for each HTTPS request/response, but the SSL session can be persisted.

Although the present invention has been described hereinabove by way of an illustrative embodiment thereof, this embodiment can be modified at will, within the scope of the present invention, without departing from the spirit and nature of the subject of the present invention.

WHATIS CLAIMED IS:

1. A method for securely associating external information available at an intermediate node with an HTTPS session comprising the steps of:

establishing a secure transport between a client and a server;

transmitting a secure request from said client to said server via said secure transport using HTTPS;

transmitting a secure response from said server to said client via said secure transport using HTTPS, said response comprising an identifier of the intermediate node, a reference to said request and a domain identifier;

establishing a first transport between said client and the intermediate node;

transmitting a first request from said client to the intermediate node using HTTP, said first request comprising said request reference and said domain identifier,

establishing a second transport between the intermediate node and said server;

transmitting a second request from the intermediate node to said server using HTTP, said second request comprising the external information, said request reference and said domain identifier;

transmitting a first response from said server to said intermediate node; and

transmitting a second response from said intermediate node to said client.

2. The method of Claim 1, wherein the external information is an MSISDN.

3. The method of Claim 1, wherein said secure transport is a SSL session.

4. The method of Claim 1, wherein said transport between said client and said intermediate node is an unsecured socket session.

5. The method of Claim 1, wherein said secured response further comprises a cookie, and wherein said unsecured domain identifier is a value of said cookie.

6. The method of Claim 5, wherein said secure response further comprises a secure domain identifier, and wherein said secure domain identifier is a value of said cookie.

7. A system for securely associating external information available at an intermediate node with an HTTPS session comprising a plurality of clients, at least one intermediate node and at least one, the system implementing the methods of Claims 1 through 6.

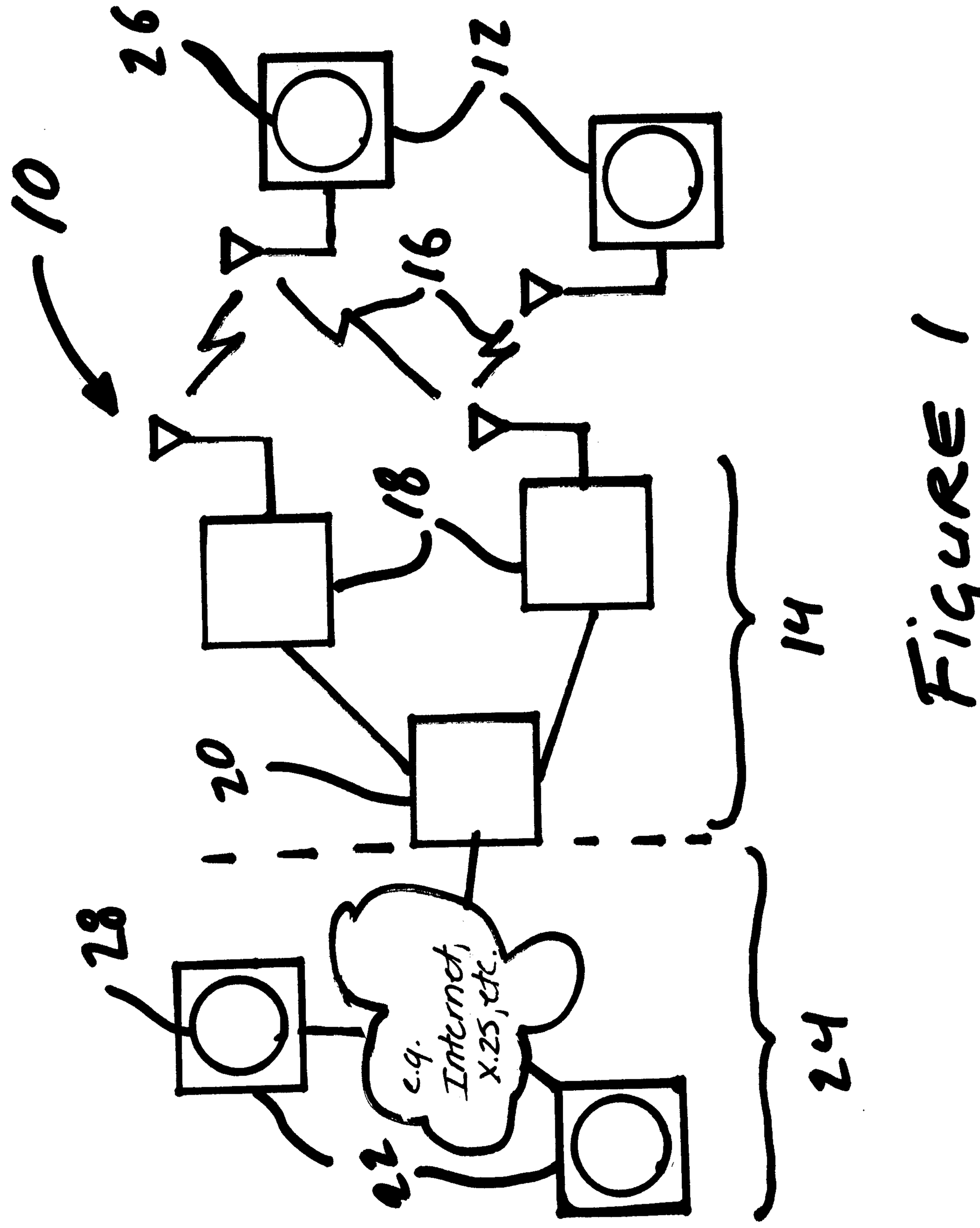


Figure 1

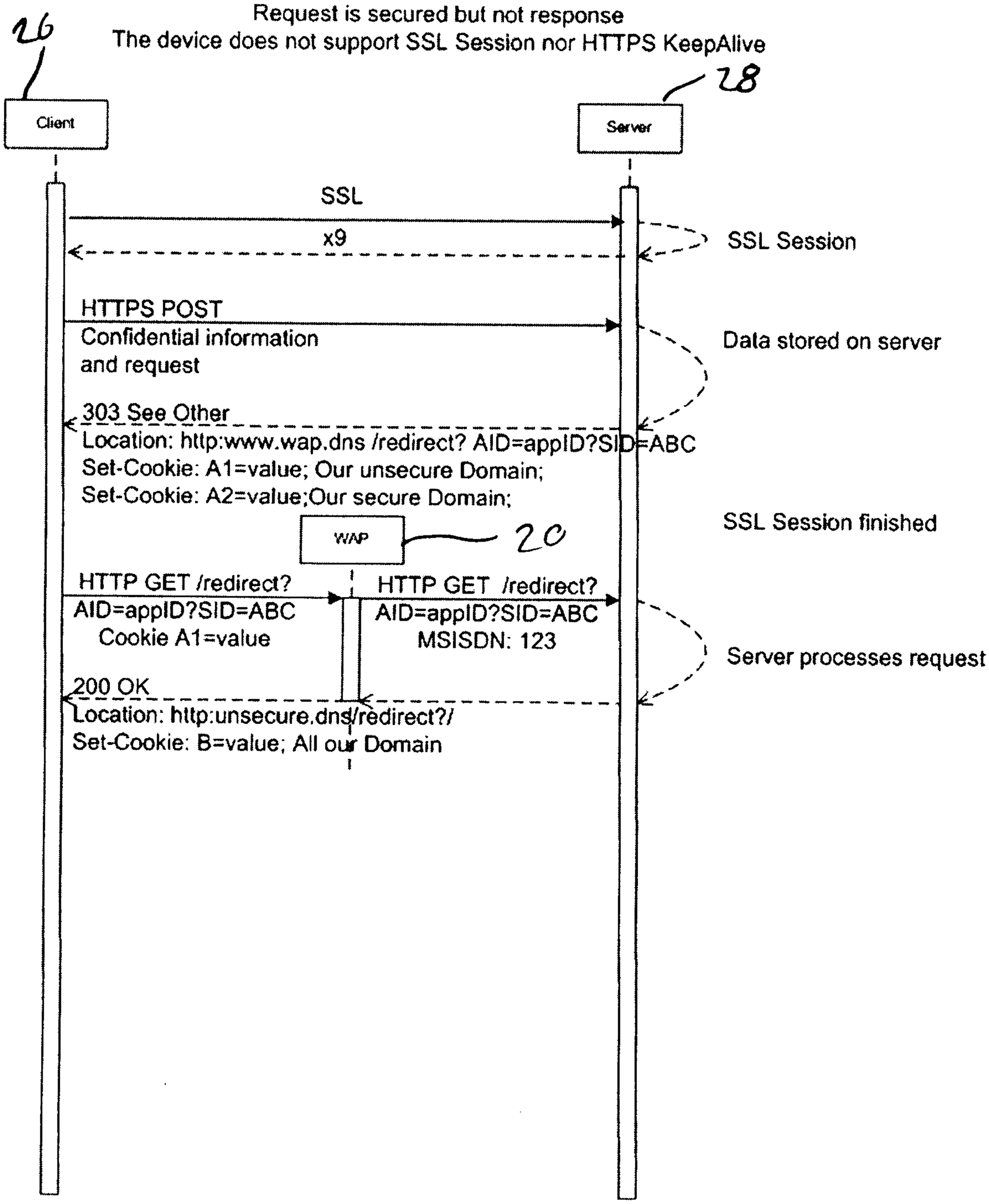

HTTPS Basic redirection
Request is secured but not response
The device does not support SSL Session nor HTTPS KeepAlive
26
Client
28
Server
SSL
x9
SSL Session
HTTPS POST
Confidential information
and request
Data stored on server
303 See Other
Location: http:www.wap.dns /redirect? AID=appID?SID=ABC
Set-Cookie: A1=value; Our unsecure Domain;
Set-Cookie: A2=value;Our secure Domain;
SSL Session finished
WAP
20
HTTP GET /redirect?
AID=appID?SID=ABC
Cookie A1=value
HTTP GET /redirect?
AID=appID?SID=ABC
MSISDN: 123
Server processes request
200 OK
Location: http:unsecure.dns/redirect?/
Set-Cookie: B=value; All our Domain

FIGURE 2

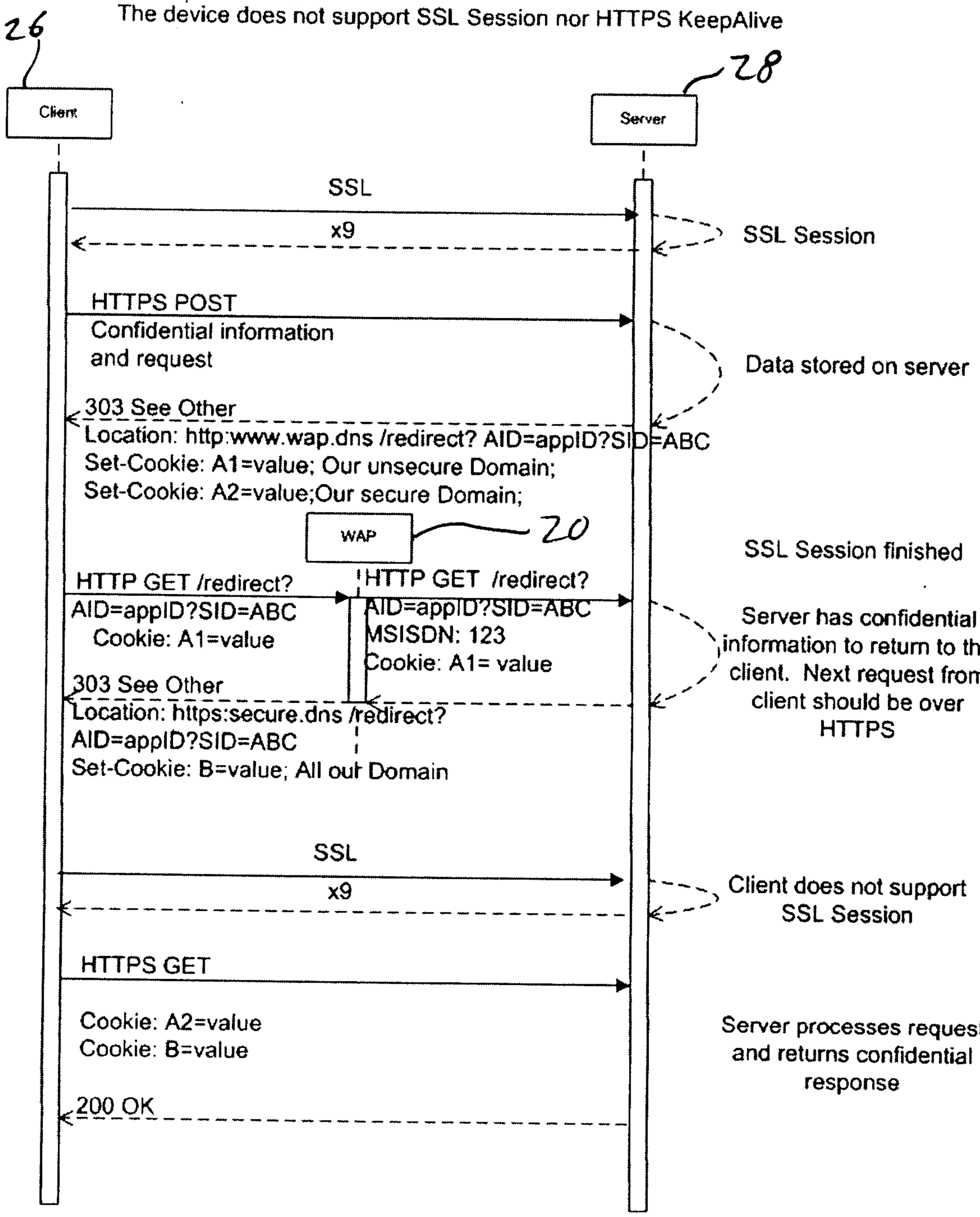

HTTPS Basic redirection
The device does not support SSL Session nor HTTPS KeepAlive
26
Client
28
Server
SSL
x9
SSL Session
HTTPS POST
Confidential information
and request
Data stored on server
303 See Other
Location: http:www.wap.dns /redirect? AID=appID?SID=ABC
Set-Cookie: A1=value; Our unsecure Domain;
Set-Cookie: A2=value;Our secure Domain;
WAP
20
SSL Session finished
HTTP GET /redirect?
AID=appID?SID=ABC
Cookie: A1=value
HTTP GET /redirect?
AID=appID?SID=ABC
MSISDN: 123
Cookie: A1= value
Server has confidential information to return to the client. Next request from client should be over HTTPS
303 See Other
Location: https:secure.dns /redirect?
AID=appID?SID=ABC
Set-Cookie: B=value; All out Domain
SSL
x9
Client does not support SSL Session
HTTPS GET
Cookie: A2=value
Cookie: B=value
Server processes request and returns confidential response
200 OK

FIGURE 3

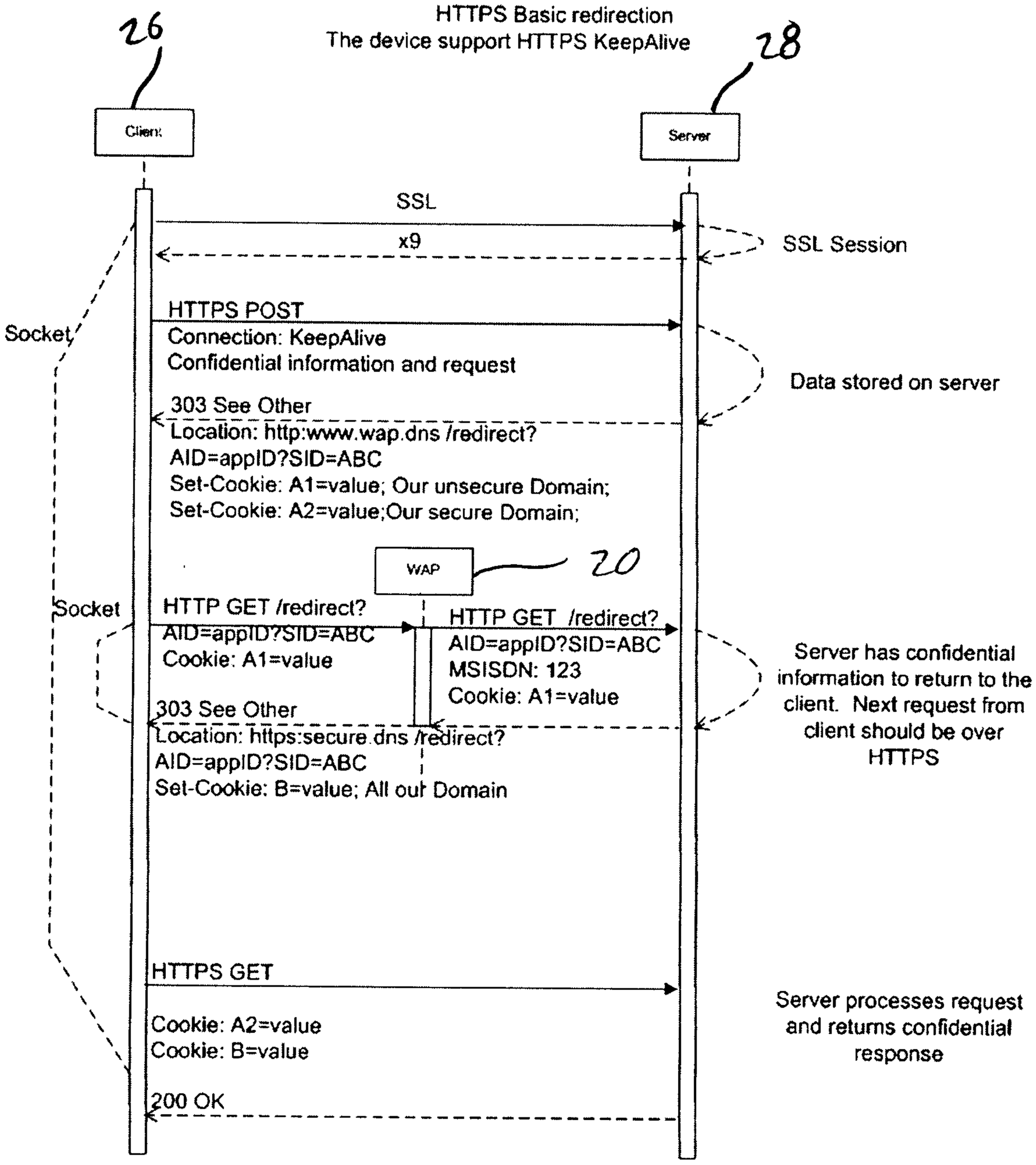

HTTPS Basic redirection
The device support HTTPS KeepAlive
26
28
Client
Server
SSL
x9
SSL Session
HTTPS POST
Connection: KeepAlive
Confidential information and request
Socket
Data stored on server
303 See Other
Location: http:www.wap.dns /redirect?
AID=appID?SID=ABC
Set-Cookie: A1=value; Our unsecure Domain;
Set-Cookie: A2=value;Our secure Domain;
WAP
20
Socket
HTTP GET /redirect?
AID=appID?SID=ABC
Cookie: A1=value
HTTP GET /redirect?
AID=appID?SID=ABC
MSISDN: 123
Cookie: A1=value
Server has confidential information to return to the client. Next request from client should be over HTTPS
303 See Other
Location: https:secure.dns /redirect?
AID=appID?SID=ABC
Set-Cookie: B=value; All out Domain
HTTPS GET
Cookie: A2=value
Cookie: B=value
Server processes request and returns confidential response
200 OK

FIGURE 4

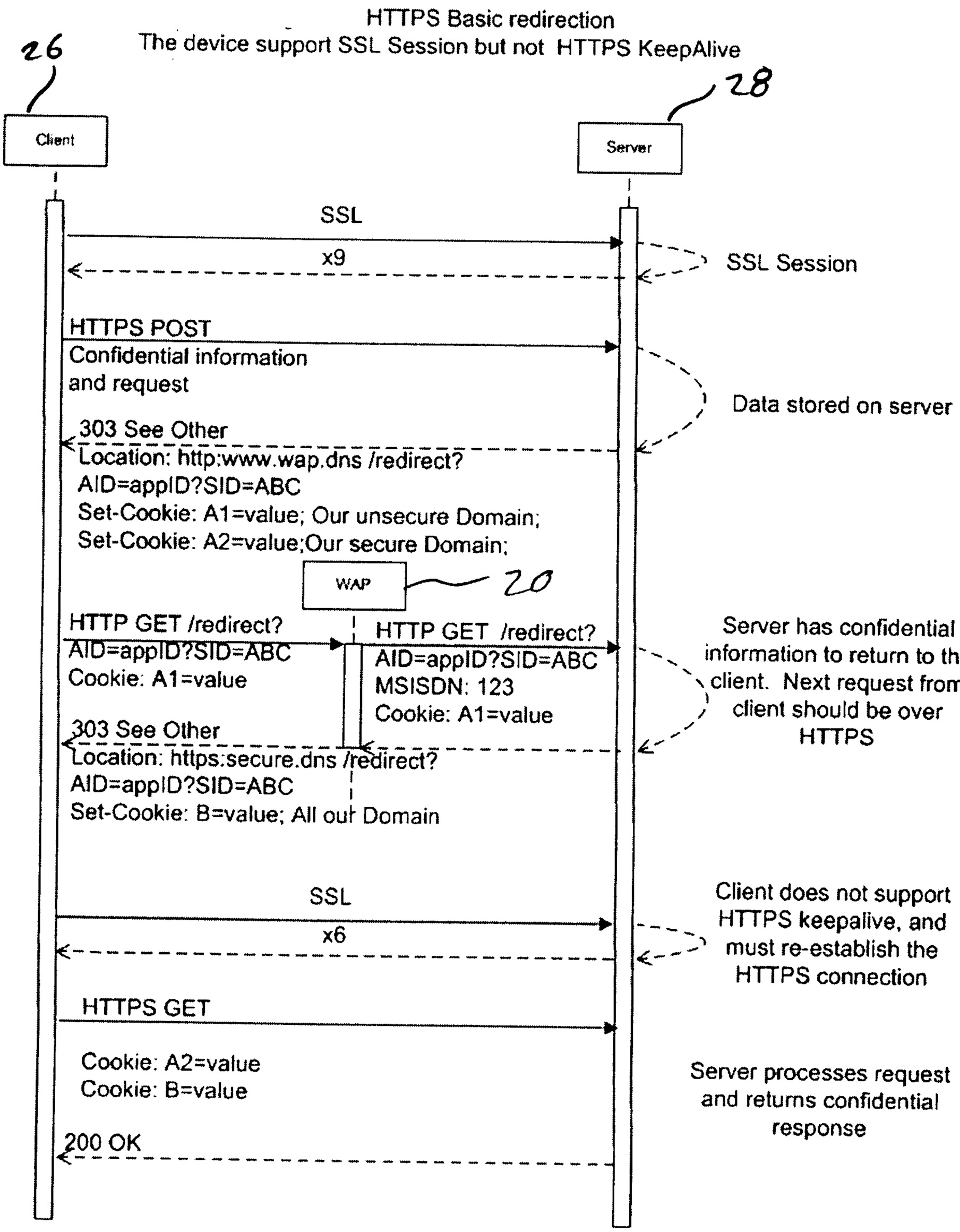
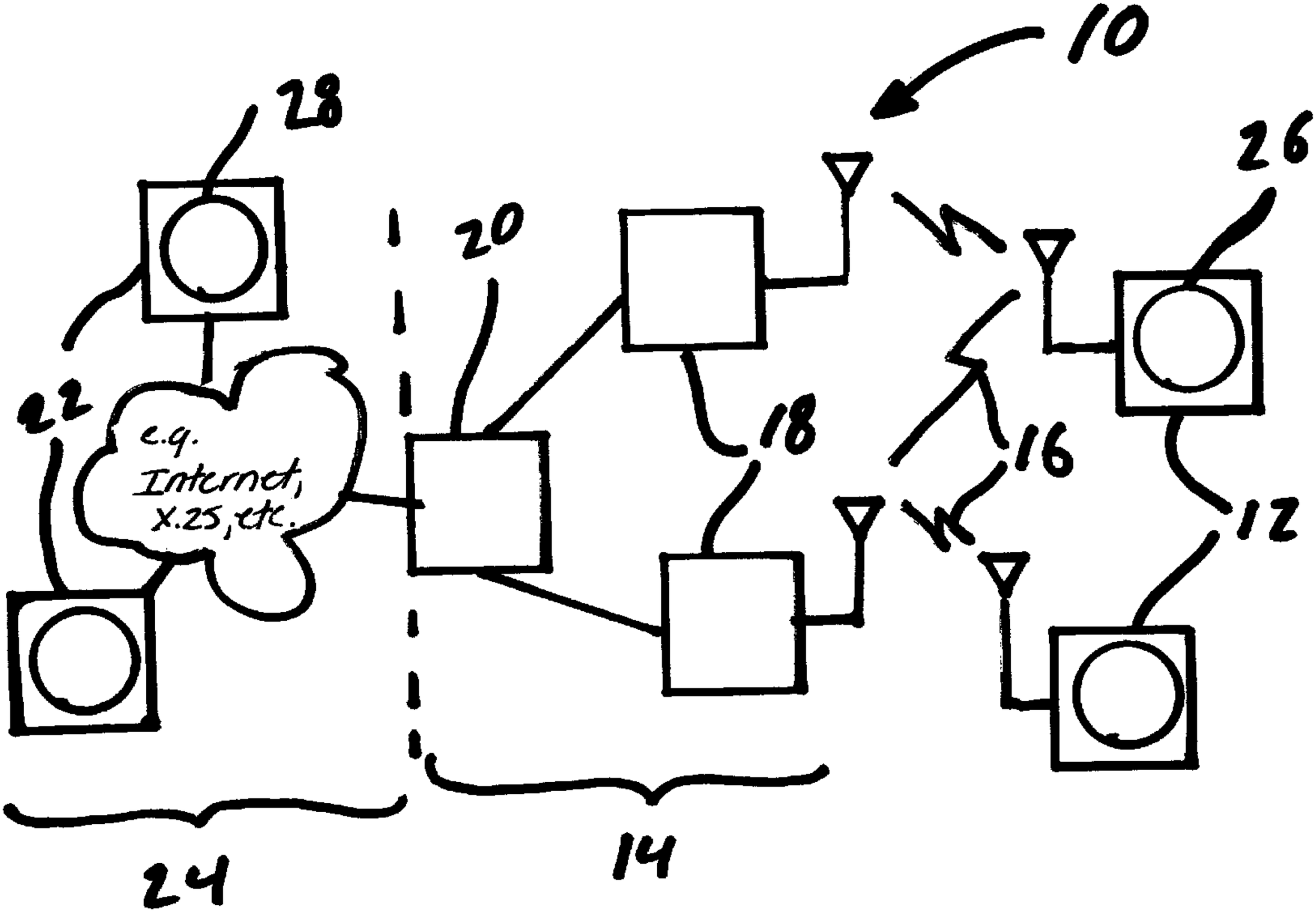

HTTPS Basic redirection
The device support SSL Session but not HTTPS KeepAlive
26
Client
28
Server
SSL
x9
SSL Session
HTTPS POST
Confidential information
and request
Data stored on server
303 See Other
Location: http:www.wap.dns /redirect?
AID=appID?SID=ABC
Set-Cookie: A1=value; Our unsecure Domain;
Set-Cookie: A2=value;Our secure Domain;
WAP
20
HTTP GET /redirect?
AID=appID?SID=ABC
Cookie: A1=value
HTTP GET /redirect?
AID=appID?SID=ABC
MSISDN: 123
Cookie: A1=value
Server has confidential information to return to the client. Next request from client should be over HTTPS
303 See Other
Location: https:secure.dns /redirect?
AID=appID?SID=ABC
Set-Cookie: B=value; All our Domain
SSL
x6
Client does not support HTTPS keepalive, and must re-establish the HTTPS connection
HTTPS GET
Cookie: A2=value
Cookie: B=value
Server processes request and returns confidential response
200 OK

FIGURE 5


10
28
26
20
22
e.g.
Internet,
X.25, etc.
18
16
12
24
14