SYSTEMS AND METHODS FOR AUTHENTICATING NETWORK MESSAGES

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application is a continuation-in-part application of U.S. Patent Application No 14/942,048, filed November 16, 2015. The entire disclosure of the above application is incorporated herein by reference.

FIELD

[0002] The present disclosure generally relates to systems and methods for use in authenticating messages, for example, network messages, including authenticating messages from clients, and further authenticating computing devices through which the messages are passed.

BACKGROUND

[0003] This section provides background information related to the present disclosure which is not necessarily prior art.

[0004] Payment networks are provided for various different types of messaging to and from clients, such as merchants, acquirers, issuers, and other entities, and further, in certain instances, among the clients. Because the messages generally include sensitive and/or confidential data, or seek access to sensitive and/or confidential data, known payment networks employ a variety of encryption techniques to protect the data, and may further dictate security conditions for messaging to and/or from the payment networks. Also, payment networks are known to employ security hierarchies, whereby as messaging progresses between different network parts or zones within the payment networks, continued authentication of the messages is needed to ensure security of the payment networks.

SUMMARY

[0004a] According to an aspect, the present disclosure refers to a computer-implemented method for use in providing authentication of an application programming interface

(API) message to a network, the method comprising: receiving, by at least one computing device, an API message from a client, the API message including a client certificate, the at least one computing device coupled between the client and an API gateway, the API message directed to one or more backend services each exposing one or more APIs to the client; appending, by the at least one computing device, the client certificate to the API message as an object; transmitting, by the at least one computing device, the appended API message to the API gateway, the API gateway associated with a plurality of recognized computing devices; validating, by the API gateway, for the appended API message, the at least one computing device based on a certificate identifying the at least one computing device as one of the recognized computing devices; validating, by the API gateway, for the appended API message, the client based on the client certificate appended to the API message; and causing a security token indicative of the client to be generated for the appended API message, when the at least one computing device and the client are validated, whereby the security token is indicative of the client and permits the API message, from the client, to be delivered to the one or more backend services.

DRAWINGS

[0005] The drawings described herein are for illustrative purposes only of selected embodiments and not all possible implementations, and are not intended to limit the scope of the present disclosure.

CLAIMS

What is claimed is:

1. A computer-implemented method for use in providing authentication of an application programming interface (API) message to a network, the method comprising:

receiving, by at least one computing device, an API message from a client, the API message including a client certificate, the at least one computing device coupled between the client and an API gateway, the API message directed to one or more backend services each exposing one or more APIs to the client;

appending, by the at least one computing device, the client certificate to the API message as an object;

transmitting, by the at least one computing device, the appended API message to the API gateway, the API gateway associated with a plurality of recognized computing devices;

validating, by the API gateway, for the appended API message, the at least one computing device based on a certificate identifying the at least one computing device as one of the recognized computing devices;

validating, by the API gateway, for the appended API message, the client based on the client certificate appended to the API message; and

causing a security token indicative of the client to be generated for the appended API message, when the at least one computing device and the client are validated, whereby the security token is indicative of the client and permits the API message, from the client, to be delivered to the one or more backend services.

2. The method of claim 1, wherein validating the at least one computing device includes validating a distinguished name of the certificate identifying the at least one computing device as consistent with the one of the recognized computing devices.

3. The method of claim 1, wherein causing the security token to be generated includes:

generating an internal security token, when the at least one computing device is validated and the client is validated;

causing a security service computing device to convert the internal security token into said security token; and

transmitting the API message including said security token to the one or more backend services indicated by said API message.

4. The method of claim 3, wherein at least one of the internal security token and said security token includes a security assertion markup language (SAML) token.

5. The method of claim 1, further comprising validating, by the at least one computing device, the client based on the client certificate, via a global access manager, prior to appending the client certificate to the API message as the object.

6. The method of claim 1, wherein the object includes an X509 object; and

wherein appending the client certificate to the API message includes appending the X509 object to a header of the API message.

7. The method of claim 1, wherein the API message includes an HTTP request; and

wherein appending the client certificate to the API message includes appending the client certificate, as an X509 object, to a header of the HTTP request.

8. The method of claim 1, wherein the client includes a merchant plug-in (MPI) associated with a 3D secure protocol; and

wherein the API message includes an authentication request.

9. The method of claim 1, further comprising terminating the API message when the at least one computing device is not validated.