

WHAT IS CLAIMED IS:

1                   1.       A computer-implemented method comprising:  
2                   receiving, via an external network by a first computer in a first low security  
3 zone of a first system, a first application programming interface (API) message from a second  
4 system for a first service provided by the first system, the first system comprising a first high  
5 security zone behind a first firewall and the first low security zone in front of the first  
6 firewall, the first low security zone connected with the external network, the second system  
7 comprising a second high security zone behind a second firewall and a second low security  
8 zone in front of the second firewall, the second low security zone being distinct from the first  
9 low security zone and connected with the external network, the first API message generated  
10 by a second computer in the second high security zone of the second system using a  
11 cryptographic algorithm and a private key associated with the second system, wherein the  
12 first and second high security zones have a greater number of firewalls between the external  
13 network than the first and second low security zones have between the external network;  
14                   authenticating, by the first computer in the first low security zone of the first  
15 system, the first API message using the cryptographic algorithm and a public key that  
16 corresponds to the private key associated with the second system; and  
17                   transmitting the authenticated first API message to a third computer in the first  
18 high security zone of the first system.

1                   2.       The method of claim 1, wherein the first API message comprises a key  
2 identifier associated with the public key, and wherein authenticating the first API message  
3 comprises retrieving the public key using the key identifier.

1                   3.       The method of claim 1, wherein the cryptographic algorithm comprises  
2 RSA-SHA2 or elliptic curve digital signature algorithm (ECDSA).

1                   4.       The method of claim 1, wherein the cryptographic algorithm comprises  
2 a hash function and a decryption function, and wherein authenticating the first API message  
3 comprises:  
4                   obtaining a signature token from the first API message;  
5                   generating data to sign based on the first API message;  
6                   applying the hash function to the data to sign to obtain a hash;

7                   applying the decryption function to at least a portion of the signature token  
8                   and the public key to obtain decrypted signature data; and  
9                   determining whether the hash matches the decrypted signature data.

1                   5.       The method of claim 4, wherein the first API message comprises a  
2                   method, a resource identifier, a message header, and a message body, and wherein generating  
3                   the data to sign based on the first API message comprises:

4                   obtaining a timestamp from the signature token;  
5                   obtaining a header hash of at least a portion of the message header;  
6                   obtaining a body hash of at least a portion of the message body; and  
7                   combining the timestamp, the header hash, the body hash, the method and the  
8                   resource identifier to generate the data to sign.

1                   6.       The method of claim 1, wherein authenticating the first API message  
2                   comprises verifying a timestamp associated with the first API message to ensure that the first  
3                   API message is received within a predetermined threshold amount of time from a time  
4                   indicated by the timestamp.

1                   7.       The method of claim 1, wherein the first API message comprises a key  
2                   identifier and authenticating the first API message comprises:

3                   retrieving one or more allowable network addresses using the key identifier;  
4                   and

5                   verifying that a network address associated with the first API message is  
6                   included in the one or more allowable network addresses.

1                   8.       The method of claim 1, wherein the third computer in the first high  
2                   security zone of the first system is configured to decrypt at least a portion of the authenticated  
3                   first API message using a shared secret to obtain decrypted message data and to validate the  
4                   decrypted message data.

1                   9.       The method of claim 8, wherein the third computer in the first high  
2                   security zone of the first system is further configured to route the authenticated first API  
3                   message to a fourth computer in the first high security zone of the first system that  
4                   implements the first service provided by the first system.

1                   10.      The method of claim 9, further comprising:

generating, by a fifth computer in the first high security zone of the first system, a second API message that corresponds to the first API message, using the cryptographic algorithm and a private key associated with the first system, wherein the second API message is authenticated by a sixth computer in the second low security zone of the second system using a public key that corresponds to the private key associated with the first system.

11. A first computer system, comprising:

a third computer in a first high security zone of the first computer system, the first computer system comprising the first high security zone behind a first firewall and a first low security zone in front of the first firewall, the first low security zone connected with an external network, the third computer comprising one or more processors configured to:

generate a first application programming interface (API) message for a second computer system, the second computer system comprising a second high security zone behind a second firewall and a second low security zone in front of the second firewall, the second low security zone being distinct from the first low security zone and connected with the external network, the first API message being generated using a cryptographic algorithm and a first private key associated with the first computer system; and

provide a first public key that that corresponds to the first private key associated with the first computer system to the second computer system, wherein the first public key is used by a fourth computer in the second low security zone of the second computer system to authenticate the first API message; and

a first computer in the first low security zone of the first computer system, the first computer comprising one or more processors configured to:

receive a second API message from the second computer system, the second API message being generated by a second computer in the second high security zone of the second computer system using the cryptographic algorithm and a second private key associated with the second computer system; and

authenticate the second API message using the cryptographic algorithm and a second public key that corresponds with the second private key associated with the second computer system,

26 wherein the first and second high security zones have a greater number of  
27 firewalls between the external network than the first and second low security zones have  
28 between the external network.

1 12. The first computer system of claim 11, wherein the one or more  
2 processors of the first computer are further configured to encrypt at least a portion of first  
3 API message using a shared secret.

1 13. The first computer system of claim 11, wherein generating the first  
2 API message comprises generating a digital signature of the first API message using the  
3 cryptographic algorithm and the first private key.

1 14. The first computer system of claim 11, wherein the one or more  
2 processors of the first computer are further configured to receive a first key identifier  
3 associated with the first public key from the second computer system, wherein the first key  
4 identifier is included in the first API message.

1 15. The first computer system of claim 11, further comprising a fifth  
2 computer comprising one or more processors configured to:  
3 receive the second public key from the second computer system; and  
4 provide a second key identifier associated with the second public key to the  
5 second computer system, wherein the second key identifier is included in the second API  
6 message.

1 16. The first computer system of claim 15, wherein authenticating the  
2 second API message comprises obtaining, by the third computer, the second key identifier  
3 from the second API message and retrieving the second public key using the second key  
4 identifier.

1 17. The first computer system of claim 15, wherein the one or more  
2 processors of the fifth computer are further configured to provide a notification to the second  
3 computer system regarding expiration of the second public key.

1 18. The first computer system of claim 11, wherein the one or more  
2 processors of the third computer are further configured to transmit the authenticated second  
3 API message to a sixth computer in the first high security zone of the first computer system,

the sixth computer being configured to decrypt at least a portion of the authenticated second API message using a shared secret.

19. A computer system, comprising:  
a memory that stores computer-executable instructions; and  
one or more processors in a low security zone of the computer system, the low security zone being in front of a firewall of the computer system, the one or more processors configured to access the memory and execute the computer-executable instructions to at least:  
receive, over an external network, an authorization request from a client of the computer system, the authorization request comprising one or more user credentials of the client, the low security zone connected with an external network;  
transmit the authorization request to a second computer in a high security zone of the computer system, the high security zone behind the firewall of the computer system, wherein the high security zone has a greater number of firewalls between the external network than the low security zone has between the external network;  
receive from the second computer in the high security zone an authorization response comprising an authorization token that is signed using a cryptographic algorithm and a private key associated with the computer system;  
transmit the authorization response to the client;  
receive a service request from the client, the service request comprising the signed authorization token;  
authenticate the service request by verifying the signed authorization token using the cryptographic algorithm and a public key that corresponds to the private key associated with the computer system; and  
transmit the authenticated service request to a third computer in the high security zone of the computer system, the third computer configured to further process the service request.

20. The computer system of claim 19, wherein the second computer is configured to encrypt the authorization token using a shared secret and the third computer is configured to decrypt the authorization token using the shared secret.

21. A computer system comprising one or more processors configured to perform the method of any one of claims 1-10.