

WHAT IS CLAIMED IS:

1. ——— A computer implemented method comprising performing, by a first computer in a first high security zone of a first system:

transmitting, over a network, a public key to be obtained by a second computer in a low security zone of a second system, wherein the public key corresponds to a private key associated with the first system, the first system comprising the first high security zone behind a first firewall and a first low security zone in front of the first firewall, the second system comprising a second high security zone behind a second firewall and a second low security zone in front of the second firewall;

receiving, over the network, a key ID that identifies the public key;

generating a first application programming interface (API) message that includes the key ID;

obtaining data to be signed from the first API message;

generating a signature token by signing the data using a cryptographic algorithm and the private key associated with the first system; and

transmitting the first API message to the second computer in the low security zone of the second system.

2. ——— The method of claim 1, wherein the public key is transmitted to another computer from which the second computer obtains the public key.

3. ——— The method of claim 1, wherein the key ID is received from the second system and is configured to be used by the second computer to retrieve the public key for authenticating the first API message.

4. ——— The method of claim 1, wherein the first API message is a request for a service provided by the second system.

5. ——— The method of claim 4, wherein the first API message invokes the service provided by the second system in a third computer of the second high security zone of the second system.

6. — The method of claim 5, wherein the data of the first API message comprises a resource identifier corresponding to the service provided by the second system, and wherein generating the signature token includes:

applying a hash function of the cryptographic algorithm to the data from the first API message, including the resource identifier, to obtain at least a portion of the signature token.

7. — The method of claim 1, wherein the first API message is a response to an API request for a service provided by the first system, and wherein the API request is received by the first computer via a third computer in a first low security zone of the first system.

8. — The method of claim 1, where the signed data includes only a portion of a header and/or body of the first API message.

9. — The method of claim 1, further comprising:
encrypting at least a portion of the first API message using a shared secret that is shared with a third computer of the second high security zone of the second system.

10. — The method of claim 9, wherein the first API message invokes a service provided by the second system in a fourth computer of the second high security zone of the second system, and wherein the third computer is configured to route a decrypted first API message to the fourth computer.

11. — A first computer system comprising:
— a first computer in a first high security zone of the first computer system, the first computer comprising one or more processors configured to:
— transmit, over a network, a public key to be obtained by a second computer in a
— low security zone of a second system, wherein the public key corresponds to a private
— key associated with 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 second system comprising a second high security zone behind a second firewall and a second low security zone in front of the second firewall;~~
~~receive, over the network, a key ID that identifies the public key;~~
~~generate a first application programming interface (API) message that includes the key ID;~~
~~obtain data to be signed from the first API message;~~
~~generate a signature token by signing the data using a cryptographic algorithm and the private key associated with the first computer system; and~~
~~transmit the first API message to the second computer in the low security zone of the second system.~~

12. The first computer system of claim 11, wherein the public key is transmitted to another computer from which the second computer obtains the public key.

13. The first computer system of claim 11, wherein the key ID is received from the second system, and wherein the key ID is configured to be used by the second computer to retrieve the public key for authenticating the first API message.

14. The first computer system of claim 11, wherein the first API message is a request for a service provided by the second system.

15. The first computer system of claim 14, wherein the one or more processors of the first computer are configured to invoke, by transmitting the first API message, the service provided by the second system in a third computer of the second high security zone of the second system.

16. The first computer system of claim 15, wherein the data of the first API message comprises a resource identifier corresponding to the service provided by the second system, and wherein generating the signature token includes applying a hash function of the cryptographic algorithm to the data from the first API message, including the resource identifier, to obtain at least a portion of the signature token.

~~17. — The first computer system of claim 11, wherein the first API message is a response to an API request for a service provided by the first computer system, and the one or more processors of the first computer are configured to receive the API request via a third computer in a first low security zone of the first computer system.~~

~~18. — The first computer system of claim 11, wherein the signed data includes only a portion of a header and/or body of the first API message.~~

~~19. — The first computer system of claim 11, wherein the one or more processors of the first computer are configured to encrypt at least a portion of the first API message using a shared secret that is shared with a third computer of the second high security zone of the second system.~~

~~20. — The first computer system of claim 19, wherein the one or more processors of the first computer are configured to invoke, using the first API message, a service provided by the second system in a fourth computer of the second high security zone of the second system, and wherein the third computer is configured to route a decrypted first API message to the fourth computer.~~

WHAT IS CLAIMED IS:

1. A computer-implemented method comprising performing, by a first computer in a first high security zone of a first system:
transmitting, over a network, a public key to be obtained by a second computer in a low security zone of a second system, wherein the public key corresponds to a private key associated with the first system, the first system comprising the first high security zone behind a first firewall and a first low security zone in front of the first firewall, the second system comprising a second high security zone behind a second firewall and a second low security zone in front of the second firewall;
receiving, over the network, a key ID that identifies the public key;
generating a first application programming interface (API) message that includes the key ID, wherein the first API message is a request for a service provided by the second system;
obtaining data to be signed from the first API message, the data comprising a resource identifier corresponding to the service provided by the second system;
generating a signature token by signing the data using a cryptographic algorithm and the private key associated with the first system, the generating comprising applying a hash function of the cryptographic algorithm to the data from the first API message, including the resource identifier, to obtain at least a portion of the signature token; and
transmitting the first API message to the second computer in the low security zone of the second system, wherein the first API message invokes the service provided by the second system in a third computer of the second high security zone of the second system.
2. The method of claim 1, wherein the public key is transmitted to another computer from which the second computer retrieves the public key.
3. The method of claim 1, wherein the key ID is received from the second system and is configured to be used by the second computer to retrieve the public key for authenticating the first API message.

4. The method of claim 1, wherein the first API message is a response to an API request for a service provided by the first system, and wherein the API request is received by the first computer via a fourth computer in the first low security zone of the first system.

5. The method of claim 1, where the signed data includes only a portion of a header and/or body of the first API message.

6. The method of claim 1, further comprising:
encrypting at least a portion of the first API message using a shared secret that is shared with a fourth computer of the second high security zone of the second system.

7. The method of claim 6, wherein the fourth computer is configured to route a decrypted first API message to the third computer.

8. A first computer system, comprising:
a first computer in a first high security zone of the first computer system, the first computer comprising one or more processors configured to:

transmit, over a network, a public key to be obtained by a second computer in a low security zone of a second system, wherein the public key corresponds to a private key associated with 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 second system comprising a second high security zone behind a second firewall and a second low security zone in front of the second firewall;

receive, over the network, a key ID that identifies the public key;
generate a first application programming interface (API) message that includes the key ID, wherein the first API message is a request for a service provided by the second system;

obtain data to be signed from the first API message the data comprising a resource identifier corresponding to the service provided by the second system;

generate a signature token by signing the data using a cryptographic algorithm and the private key associated with the first computer system, the generating comprising applying a hash function of the cryptographic algorithm to the data from the first API

message, including the resource identifier, to obtain at least a portion of the signature token;
and

transmit the first API message to the second computer in the low security zone
of the second system, wherein the first API message invokes the service provided by the
second system in a third computer of the second high security zone of the second system.

9. The system of claim 8, wherein the public key is transmitted to another
computer from which the second computer retrieves the public key.

10. The system of claim 8, wherein the key ID is received from the second
system and is configured to be used by the second computer to retrieve the public key for
authenticating the first API message.

11. The system of claim 8, wherein the first API message is a response to an
API request for a service provided by the first computer system, and wherein the API request is
received by the first computer via a fourth computer in the first low security zone of the first
computer system.

12. The system of claim 8, wherein the signed data includes only a portion of
a header and/or body of the first API message.

13. The system of claim 8, wherein the one or more processors of the first
computer are further configured to encrypt at least a portion of the first API message using a
shared secret that is shared with a fourth computer of the second high security zone of the second
system.

14. One or more non-transitory computer-readable storage media storing
a plurality of instructions that when executed cause one or more processors of a first computer in a
first high security zone of a first system to perform:

transmitting, over a network, a public key to be obtained by a second computer in
a low security zone of a second system, wherein the public key corresponds to a private key
associated with the first system, the first system comprising the first high security zone behind a
first firewall and a first low security zone in front of the first firewall, the second system

comprising a second high security zone behind a second firewall and a second low security zone in front of the second firewall;

receiving, over the network, a key ID that identifies the public key;

generating a first application programming interface (API) message that includes the key ID, wherein the first API message is a request for a service provided by the second system;

obtaining data to be signed from the first API message the data comprising a resource identifier corresponding to the service provided by the second system;

generating a signature token by signing the data using a cryptographic algorithm and the private key associated with the first system, the generating comprising applying a hash function of the cryptographic algorithm to the data from the first API message, including the resource identifier, to obtain at least a portion of the signature token; and

transmitting the first API message to the second computer in the low security zone of the second system, wherein the first API message invokes the service provided by the second system in a third computer of the second high security zone of the second system.

15. The one or more non-transitory computer-readable storage media of claim 14, wherein the public key is transmitted to another computer from which the second computer retrieves the public key.

16. The one or more non-transitory computer-readable storage media of claim 14, wherein the key ID is received from the second system and is configured to be used by the second computer to retrieve the public key for authenticating the first API message.

17. The one or more non-transitory computer-readable storage media of claim 14, wherein the first API message is a response to an API request for a service provided by the first system, and wherein the API request is received by the first computer via a fourth computer in the first low security zone of the first system.

18. The one or more non-transitory computer-readable storage media of claim 14, wherein the signed data includes only a portion of a header and/or body of the first API message.

19. The one or more non-transitory computer-readable storage media of claim 14, wherein the one or more processors of the first computer are further configured to encrypt at least a portion of the first API message using a shared secret that is shared with a fourth computer of the second high security zone of the second system.

20. The one or more non-transitory computer-readable storage media of claim 19, wherein the fourth computer is configured to route a decrypted first API message to the third computer.