Claims

1. A computer-implemented method for controlling access to a first computer system that controls operations of an intermodal shipping container, the method comprising:

generating a secret value at the first computer system;

sharing the secret value with associated computer systems;

choosing a time length for validity;

computing a derived key based on the secret value; and

controlling remote access to the first computer system based on the derived key and a unique identifier associated with the first computer system, wherein the unique identifier is associated with the intermodal shipping container;

wherein remote access to the first computer system is controlled by:

displaying the derived key on the first computer system, allowing a user to read and enter the derived key onto a remote computer system;

computing a passkey based on the derived key and unique identidier;

transmitting the passkey to the first computer system, the first computer system comparing the transmitted passkey with a locally generated one; and

receiving a session token from the first computer system if the comparison results in a match.

2. The computer-implemented method of claim 1 wherein:

the unique identifier is a serial number associated with the intermodal shipping container.

3. The computer-implemented method of claim 1 wherein:

the associated computer systems include computer systems operated by a common entity.

4. The computer-implemented method of claim 1 wherein:

the derived key is generated using a key derivation function.

5. A computer-implemented method for controlling access to a computer system comprising:

generating a secret value at a first computer system;

sharing the secret value with associated computer systems;

choosing a time length for validity;

computing a derived key based on the secret value;

controlling remote access to the computer system based on the derived key and a unique identifier associated with the first computer system;

validating one or more certificates received from a remote computer system; and

transmitting a session token to the remote computer system, in the case where the one or more certificates are validated.

6. The computer-implemented method of claim 5 further comprising:

granting access to the remote computer system based on receiving the session token.

7. A system for controlling access to a first computer system that controls operations of an intermodal shipping container, the system comprising:

a processor;

memory;

the processor configured to perform a method comprising:

generating a secret value at the first computer system;

sharing the secret value with associated computer systems;

choosing a time length for validity;

computing a derived key based on the secret value; and

controlling remote access to the first computer system based on the derived key and a unique identifier associated with the first computer system, wherein the unique identifier is associated with the intermodal shipping container;

wherein remote access to the first computer system is controlled by:

displaying the derived key on the first computer system, allowing a user to read and enter the derived key onto a remote computer system;

computing a passkey based on the derived key and unique identifier;

transmitting the passkey to the first computer system, the first computer system comparing the transmitted passkey with a locally generated one; and

receiving a session token from the first computer system if the comparison results in a match.

8. The system of claim 7 wherein:

the unique identifier is a serial number associated with the intermodal shipping container.

9. The system of claim 7 wherein:

the associated computer systems include computer systems operated by a common entity.

10. The system of claim 7 wherein:

the derived key is generated using a key derivation function.

11. A system for controlling access to a computer system comprising:

a processor;

memory;

the processor configured to perform a method comprising:

generating a secret value at a first computer system;

sharing the secret value with associated computer systems;

choosing a time length for validity;

computing a derived key based on the secret value;

controlling remote access to the computer system based on the derived key and a unique identifier associated with the first computer system;

validating one or more certificates received from a remote computer system; and

transmitting a session token to the remote computer system, in the case where the one or more certificates are validated.

12. The system of claim 11 wherein the method further comprises:

granting access to the remote computer system based on receiving the session token.

13. A computer-implemented method for gaining remote access to a first computer system comprising:

accepting a derived key and a unique identifier as an input at a remote computer system;

computing a passkey based on the derived key and the unique identifier;

transmitting the passkey to the first computer system;

receiving a session token from the first computer system;

establishing a secure session with the first computer system using the session token;

wherein transmitting the passkey to the first computer system further comprises transmitting one or more certificates to the computer system;

wherein the one or more certificates include a customer certificate and a mobile certificate.

14. A computer-implemented method for gaining remote access to a first computer system comprising:

accepting a derived key and a unique identifier as an input at a remote computer system;

computing a passkey based on the derived key and the unique identifier;

transmitting the passkey to the first computer system;

receiving a session token from the first computer system;

establishing a secure session with the first computer system using the session token;

wherein transmitting the passkey to the first computer system further comprises transmitting one or more certificates to the first computer system;

wherein the one or more certificates are received from a certificate-granting authority upon proof of authorization.