

CLAIMS

1. A computer-implemented method for distributing a private signature key between authorization instances, the computer-implemented method comprising:
 - registering a plurality of authorization instances in a configuration file by providing a registration to the configuration, the authorization instances participating in a common service;
 - generating host instance key pairs for each of the authorization instances, wherein each of the host instance key pairs include a public host key and a private host key;
 - storing the public host keys in a shared database;
 - electing one of the authorization instances to be a signature key leader instance;
 - generating, by the signature key leader instance, a signature key pair, wherein the signature key pair includes a public signature key and a private signature key;
 - storing the public signature key in the shared database;
 - transmitting an encrypted private signature key to a requesting authorization instance of the authorization instances, wherein the private signature key is encrypted using the public host key corresponding to the requesting authorization instance; and
 - decrypting, by the requesting authorization instance, the encrypted private signature key using the private host key generated by the requesting authorization instance.
2. The computer-implemented method of claim 1, wherein transmitting the encrypted private signature key comprises:
 - detecting, by the requesting authorization instance, the public signature key stored in the shared database;

requesting, by the requesting authorization instance, the private signature key from the signature key leader instance;

validating the request made to the signature key leader instance by examining a source IP address of the request;

retrieving, upon validating the request, the public host key corresponding to the requesting authorization instance from the shared database;

encrypting the private signature key using the public host key; and

transmitting the encrypted private signature key to the requesting authorization instance.

3. The computer-implemented method of claim 2, wherein validating the request comprises:

retrieving a registration relating to the requesting authorization instance from the configuration file; and

verifying the source IP address of the request matches a stored IP address of the requesting authorization instance located in the registration.

4. The computer-implemented method of one of claims 1 to 3, further comprising:

retrieving a registration for the requesting authorization instance from the configuration file, the registration includes a hostname of the requesting authorization instance;

providing the encrypted private signature key via a callback at the hostname of the requesting authorization instance.

5. The computer-implemented method of one of claims 1 to 4, further comprising:

detecting the signature key leader instance is no longer responsive; and

electing a new signature key leader instance from the authorization instances.

6. The computer-implemented method of one of claims 1 to 5, further comprising:

performing a rollover of the signature key pair to generate a new signature key pair; and

adding a new public signature key to the shared database.

7. The computer-implemented method of one of claims 1 to 6, wherein the signature key pair is stored in memory of the signature key leader instance.

8. A non-transitory computer-readable storage medium having stored thereon instruction for controlling a computer system to:

register a plurality of authorization instances in a configuration file by providing a registration to the configuration, the authorization instances participating in a common service;

generate host instance key pairs for each of the authorization instances, wherein each of the host instance key pairs include a public host key and a private host key;

store the public host keys in a shared database;

elect one of the authorization instances to be a signature key leader instance;

generate a signature key pair by the signature key leader instance, wherein the signature key pair includes a public signature key and a private signature key;

store the public signature key in the shared database; and

transmit an encrypted private signature key to a requesting authorization instance of the authorization instances, wherein the private signature key is encrypted using the public host key corresponding to the requesting authorization instance to generate the encrypted private signature key.

9. The non-transitory computer-readable storage medium of claim 8, wherein transmit the encrypted private signature key comprises instructions to cause the computer system to:

detect, by the requesting authorization instance, the public signature key in the shared database;

request, by the requesting authorization instance, the private signature key from the signature key leader instance;

validate the request made to the signature key leader instance by examining a source IP address of the request;

retrieve, upon validating the request, the public host key corresponding to the requesting authorization instance from the shared database;

encrypt the private signature key using the public host key; and

transmit the encrypted private signature key to the requesting authorization instance.

10. The non-transitory computer-readable storage medium of claim 9, wherein validate the request comprises instructions to cause the computer system to:

retrieve a registration for the requesting authorization instance from the configuration file; and

verify the source IP address of the request matches a stored IP address of the requesting authorization instance located in the registration.

11. The non-transitory computer-readable storage medium of one of claims 8 to 10, further comprising instructions to cause the computer system to:

retrieve a registration for the requesting authorization instance from the configuration file, the registration includes a hostname of the requesting authorization instance;

provide the encrypted private signature key via a callback at the hostname of the requesting authorization instance.

12. The non-transitory computer-readable storage medium of one of claims 8 to 11, further comprising instructions to cause the computer system to:

detect the signature key leader instance being no longer responsive; and

elect a new signature key leader instance from the authorization instances.

13. The non-transitory computer-readable storage medium of one of claims 8 to 12, further comprising instructions to cause the computer system to:

perform a rollover of the signature key pair to generate a new signature key pair; and

add a new public signature key to the shared database.

14. The non-transitory computer-readable storage medium of one of claims 8 to 13, wherein the signature key pair is stored in memory of the signature key leader instance.

15. A computer system for distributing a private signature key between authorization instances, the computer system comprising:

a data processing component;

a physical memory; and

local data storage having stored thereon computer executable program code, which when executed by the data processing component causes the data processing component to:

register a plurality of authorization instances in a configuration file by providing a registration to the configuration, the authorization instances participating in a common service;

generate host instance key pairs for each of the authorization instances, wherein each of the host instance key pairs include a public host key and a private host key;

store the public host keys in a shared database;

elect one of the authorization instances to be a signature key leader instance;

generate a signature key pair by the signature key leader instance, wherein the signature key pair includes a public signature key and a private signature key;

store the public signature key in the shared database; and

transmit an encrypted private signature key to a requesting authorization instance of the authorization instances, wherein the private signature key is encrypted using the public host key corresponding to the requesting authorization instance to generate the encrypted private signature key.

16. The computer system of claim 15, wherein transmit the encrypted private signature key causes the data processing component to:

detect, by the requesting authorization instance, the public signature key in the shared database;

request, by the requesting authorization instance, the private signature key from the signature key leader instance;

validate the request made to the signature key leader instance by examining a source IP address of the request;

retrieve, upon validating the request, the public host key corresponding to the requesting authorization instance from the shared database;

encrypt the private signature key using the public host key; and

transmit the encrypted private signature key to the requesting authorization instance.

17. The computer system of claim 16, wherein validate the request causes the data processing component to:

retrieving a registration for the requesting authorization instance from the configuration file; and

verifying the source IP address of the request matches a stored IP address of the requesting authorization instance located in the registration.

18. The computer system of one of claims 15 to 17, further comprising:

retrieve a registration for the requesting authorization instance from the configuration file, the registration includes a hostname of the requesting authorization instance;

provide the encrypted private signature key via a callback at the hostname of the requesting authorization instance.

19. The computer system of one of claims 15 to 18 further comprising:

detect the signature key leader instance being no longer responsive; and

elect a new signature key leader instance from the authorization instances.

20. The computer system of one of claims 15 to 19, further comprising:

perform a rollover of the signature key pair to generate a new signature key pair; and

add a new public signature key to the shared database.