

CLAIMS

1. A method for key federation between a first enterprise and a second enterprise, the method comprising:
 - determining, by a local key orchestration device associated with the first enterprise, mutually agreed policies for encryption objects used for communication between a first communication device of the first enterprise and a second communication device of the second enterprise, wherein the mutually agreed policies are mutually agreed to by the local key orchestration device and a foreign key orchestration device associated with the second enterprise for evaluating the communication;
 - managing, by the local key orchestration device, the encryption objects based on the mutually agreed policies; and
 - distributing, by the local key orchestration device, the encryption objects to at least one of the first communication device or the second communication device to establish the communication.
2. The method of claim 1, wherein determining the mutually agreed policies comprises:
 - providing, by the local key orchestration device, first trust policy information to the foreign key orchestration device; and
 - receiving, by the local key orchestration device, second trust policy information from the foreign key orchestration device.
3. The method of claim 2, wherein determining the mutually agreed policies further comprises determining the mutually agreed policies based on one or more of the first trust policy information or the second trust policy information.
4. The method of claim 2, wherein each of the first trust policy information and the second trust policy information comprises one or more of configurations, settings, extent of trust, and the mutually agreed policies.
5. The method of claim 1, wherein managing the encryption objects comprises evaluating, by the local key orchestration device, the encryption objects against the mutually agreed policies.

6. The method of claim 5, wherein managing the encryption objects further comprises further evaluating, by the local key orchestration device, the encryption objects against first policies in addition to the mutually agreed policies.

7. The method of claim 5, wherein managing the encryption objects further comprises distributing the encryption objects to the first communication device and the second communication device in response to determining that the encryption objects are acceptable based on the mutually agreed policies.

8. The method of claim 5, wherein managing the encryption objects further comprises sending the encryption objects to the foreign key orchestration device to be checked, by the foreign key orchestration device, against second policies in addition to the mutually agreed policies.

9. The method of claim 1, further comprising storing the mutually agreed policies.

10. A non-transitory computer-readable medium having computer-readable instructions such that, when executed, causes a processor of a local key orchestration device of a first enterprise to:

determine mutually agreed policies for encryption objects used for communication between a first communication device of the first enterprise and a second communication device of a second enterprise, wherein the mutually agreed policies are mutually agreed to by the local key orchestration device and a foreign key orchestration device associated with the second enterprise for evaluating the communication;

manage the encryption objects based on the mutually agreed policies; and

distribute the encryption objects to at least one of the first communication device or the second communication device to establish the communication.

11. The non-transitory computer-readable medium of claim 10, wherein the processor of the local key orchestration device of the first enterprise determines the mutually agreed policies by:

providing, by the local key orchestration device, first trust policy information to the foreign key orchestration device; and

receiving, by the local key orchestration device, second trust policy information from the foreign key orchestration device.

12. The non-transitory computer-readable medium of claim 11, wherein determining the mutually agreed policies further comprises determining the mutually agreed policies based on one or more of the first trust policy information or the second trust policy information.

13. The non-transitory computer-readable medium of claim 11, wherein each of the first trust policy information and the second trust policy information comprises one or more of configurations, settings, extent of trust, and the mutually agreed policies.

14. The non-transitory computer-readable medium of claim 10, wherein managing the encryption objects comprises evaluating, by the local key orchestration device, the encryption objects against the mutually agreed policies.

15. The non-transitory computer-readable medium of claim 14, wherein managing the encryption objects further comprises further evaluating, by the local key orchestration device, the encryption objects against first policies in addition to the mutually agreed policies.

16. The non-transitory computer-readable medium of claim 14, wherein managing the encryption objects further comprises distributing the encryption objects to the first communication device and the second communication device in response to determining that the encryption objects are acceptable based on the mutually agreed policies.

17. The non-transitory computer-readable medium of claim 15, wherein managing the encryption objects further comprises sending the encryption objects to the foreign key orchestration device to be checked, by the foreign key orchestration device, against second policies in addition to the mutually agreed policies.

18. The non-transitory computer-readable medium of claim 10, wherein processor of the local key orchestration device of the first enterprise is configured to further store the mutually agreed policies.

19. A local key orchestration device associated with a first enterprise, comprising:
memory; and

a processor configured to:

determine mutually agreed policies for encryption objects used for communication between a first communication device of the first enterprise and a second communication device of a second enterprise, wherein the mutually agreed policies are mutually agreed to by the local key orchestration device and a foreign key orchestration device associated with the second enterprise for evaluating the communication;

manage by the local key orchestration device, the encryption objects based on the mutually agreed policies; and

distribute the encryption objects to at least one of the first communication device or the second communication device to establish the communication.

20. The local key orchestration device of claim 19, wherein the processor determines the mutually agreed policies by:

providing first trust policy information to the foreign key orchestration device;

and

receiving second trust policy information from the foreign key orchestration device.

21. The method of claim 1, further comprising:

determining that the encryption objects are acceptable based on the mutually agreed policies; and

distributing the same encryption objects to at least one of the first communication device or the second communication device to establish the communication.