

WHAT IS CLAIMED IS:

1. A process for orchestrating a security object, the process comprising:
 - defining and storing a plurality of policies in a database coupled to a policy engine;
 - receiving, by the policy engine, the security object for distributing at least one communication device and at least one object attribute associated with the security object;
 - determining, with the policy engine, acceptability of the security object based, at least in part, on the at least one object attribute and at least one of the plurality of policies corresponding to the at least one object attribute; and
 - distributing the same security object to the at least one communication device associated with the policy engine in response to the security object being determined to be acceptable, wherein the at least one communication device establishes communication based, at least in part, on the security object.
2. The process of claim 1, wherein the security object is an encryption key.
3. The process of claim 1, wherein the at least one object attribute comprise characteristics of at least one of the security object, a first device generating the security object, a second device transmitting the security object, a third device receiving the security object, a first user associated with the first device, a second

user associated with the second device, and a third user associated with the third device.

4. The process of claim 1, wherein the at least one object attribute comprises at least one of a security object size, time when the security object is generated, geo-location where the security object is generated, classification of the security object, role associated with a key source, role associated with a source device, and role associated with a target device.
5. The process of claim 4, wherein the plurality of policies comprises accepting the security object when the security object size is within a predetermined size range.
6. The process of claim 4, wherein the plurality of policies comprises accepting the security object when the security object is generated within a predetermined time interval.
7. The process of claim 4, wherein the plurality of policies comprises accepting the security object when the geo-location where the security object is generated is within a predetermined area.
8. The process of claim 4, wherein the plurality of policies comprises accepting the security object when the classification of the security object is associated with a predetermined security object classification group.

9. The process of claim 4, wherein the plurality of policies comprises accepting the security object when the role associated with the key source, the source device, or the target device is associated with a predetermined group of roles.
10. The process of claim 1, further comprising:
 - transmitting a rejection indicator to a key source; and
 - transmitting a hint informing inadequacies of the security object to the key source, wherein the security object is received from the key source.
11. The process of claim 1, wherein the receiving, by the policy engine, the security object comprises:
 - receiving, by the policy engine, a request to generate the security object;
 - and
 - generating, by the policy engine, the security object.
12. A process for orchestrating a security object, the process comprising:
 - defining and storing a first plurality of policies in a first database of a first key orchestration device, the first database being associated with a first enterprise;
 - receiving, with the first key orchestration device associated with the first enterprise, the security object for distributing to at least one communication device and at least one object attribute associated with the security object from a second key orchestration device associated with a second enterprise;

determining, with the first key orchestration device, acceptability of the security object based, at least in part, on the at least one object attribute and at least one of the first plurality of policies corresponding to the at least one object attribute; and

distributing the same security object to a first communication device associated with the first enterprise.

13. The process of claim 12, further comprising defining and storing a second plurality of policies in a second database of the second key orchestration device, wherein at least a first portion of the first plurality of policies and a second portion the second plurality of policies is the same.

14. The process of claim 12, further comprising:

transmitting, from the first key orchestration device to the second key orchestration device, the security object; and

distributing the security object to a second communication device associated with the second enterprise, wherein the first communication device and the second communication device may establish communication based on the security object.

15. The process of claim 13, further comprising:

transmitting, from the first key orchestration device to the second key orchestration device, the security object;

determining, with the second key orchestration device, the acceptability of the security object based, at least in part, on the at least one object attribute and at least one of the second plurality of policies corresponding to the at least one object attribute; and

distributing the security object to a second communication device associated with the second enterprise, wherein the first communication device and the second communication device may establish communication based on the security object.

16. The process of claim 12, wherein the receiving the security object and at least one object attribute associated with the security object from a second key orchestration device comprises:

receiving, by the first key orchestration device from the second key orchestration device, a request to generate the security object; and

generating, with a key source associated with the first enterprise, the security object in response to the request.

17. A non-transitory computer-readable medium comprising computer-readable instructions such that, when executed, causes a processor to:

define a plurality of policies in a database;

receive the security object for distributing to at least one communication device and at least one object attribute associated with the security object;

determine acceptability of the security object based, at least in part, on the at least one object attribute and at least one of the plurality of policies corresponding to the at least one object attribute; and

distribute the same security object to the at least one communication device associated with the processor in response to the security object being determined to be acceptable, wherein the at least one communication device establishes communication based, at least in part, on the security object.

18. The non-transitory computer-readable medium of claim 17, wherein the security object is an encryption key.
19. The non-transitory computer-readable medium of claim 17, wherein the at least one object attribute comprises at least one of a security object size, time when the security object is generated, geo-location where the security object is generated, classification of the security object, role associated with a key source, role associated with a source device, and role associated with a target device.
20. The non-transitory computer-readable medium of claim 17, wherein the plurality of policies comprises accepting the security object when at least one of the security object size is within a predetermined size range, the time when the security object is generated is within a predetermined time interval, the geo-location where the security object is generated is within a predetermined area, the classification of the security object is included in a predetermined security object

classification group, and the role associated with the key source, the source device, or the target device is associated with a predetermined group of roles.

21. The process of claim 1, wherein the at least one object attribute comprises cryptographic characteristics of the security object.
22. The process of claim 1, wherein the at least one object attribute comprises cryptographic algorithms of the security object.